NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

October 18, 2019

What's trending on NP Privacy Partner

The Ninth Circuit indicates that information on public LinkedIn profiles is fair game and the California governor signs seven bills related to data security and privacy. Here's what's trending in data privacy and cybersecurity.

Consumer Privacy

Ninth Circuit Indicates that Information on Public LinkedIn Profiles is Fair Game for Automated Data Scraping Bots Under the CFAA

Is the use of automated "data-scraping" bots to collect information from public LinkedIn profiles fair game under the Computer Fraud and Abuse Act (CFAA)? According to the Ninth Circuit's recent ruling in *hiQ Labs, Inc. v. LinkedIn Corporation*, No. 17-16783, 2019 WL 4251889 (9th Cir. Sept. 9, 2019), the answer is likely "yes."

In *hiQ Labs*, LinkedIn sent data analytics company hiQ a cease-and-desist letter demanding that hiQ stop scraping data from LinkedIn users' public profiles and asserting that continuation of the practice would constitute a violation of the CFAA. hiQ, in turn, sought a preliminary injunction to enjoin LinkedIn from invoking the CFAA against it.

The CFAA, codified at 18 U.S.C. § 1030, prohibits the intentional accessing of a protected computer "without authorization" in order to obtain information from it. The Ninth Circuit considered the meaning of the phrase "without authorization" and determined that its use in the statute is meant to protect against the digital equivalent of "breaking and entering." As such, simply collecting publicly available data from a website like LinkedIn does not give rise to a CFAA violation. The court rather indicated that the CFAA is violated only "when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer."

Applying this framework, the court found that there is a serious question as to whether hiQ's data-scraping practices violate the CFAA, and granted hiQ's motion for a preliminary injunction. It noted that LinkedIn does not claim to own the information that its users share on their public profiles and that such information is available without a username or password to anyone with access to a web browser. The court also rejected LinkedIn's argument that an injunction would threaten the privacy of its members, finding "little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly . . ."

The court's decision at this stage of litigation is certainly encouraging for hiQ and others engaged in similar data collection practices. The NP Privacy Partner team will continue to monitor developments in this case, but in the meantime: (i) companies seeking to protect user data should ensure that protective measures, such as required usernames and passwords, are in place to create a clear barrier between public data and that which is accessed without authorization, and (ii) LinkedIn users should be aware that information posted to their public profiles may very well end up in the hands of third-party data collectors. – *Jenny L. Holmes*

Special thanks to James Ingram for his contributions to this post.

California governor signs seven bills related to data security and privacy

On September 16, 2019, we reported on a number of bills passed by the California Legislature in the final days of the session, amending the California Consumer Privacy Act. On October 13, 2019, Governor Gavin Newsom signed those bills into law. To recap briefly, they are:

AB 25: Exempts from the scope of the Act information collected in an employment context, i.e., information collected in a job application, or from employees, directors, business owners, medical staff, or contractors. However, the private right of action for negligently allowing the disclosure of such information in Civil Code 1798.150 still applies.

AB 874: Simplifies the definition of "publicly available information," which does not count as "personal information" under the Act. Eliminates the restriction that information obtained from a public source is only exempt from the definition of personal information if it is used for the same purpose that it was gathered by the public entity.

AB 1146: Exempts information maintained or exchanged between an auto dealer and a manufacturer for warranty or recall purposes from certain obligations under the Act. Such information cannot be the subject of a request to delete, and sharing of the information between a dealer and manufacturer does not trigger an obligation to disclose it as a "sale" of such information.

AB 1202: Adds new sections Civil Code 1798.99.80-82. Requires all data brokers to register with the attorney general. A data broker is any business that knowingly collects and sells (broadly defined) personal information regarding persons with which it has no direct relationship.

AB 1355: Exempts deidentified and aggregate information from the definition of "consumer information" in the Act; also clarifies the interrelationship of the Act and the Fair Credit Reporting Act.

AB 1564: Streamlines the methods businesses must make available to consumers to make requests to disclose their personal information. A business that operates exclusively online and has a relationship with the consumer is only required to make a single online method available for such requests. However, a business that maintains a website must include the website as one of the methods to receive such requests.

In addition, the governor signed AB 1130, which amends the state's data breach notification law. It revises the definition of personal information for breach notification purposes to add specified unique biometric data and tax identification numbers, passport numbers, military identification numbers, and unique identification numbers issued on a government document in addition to the existing categories that already include driver's licenses and California identification cards. Upon a breach of biometric data, the breach notice now must include instructions on how the consumer can notify entities who

may be relying on such data for identification purposes to let them know that it is no longer secure. – *Karl Belgum*

For more information, please contact:

- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494
- Karl Belgum at **kbelgum@nixonpeabody.com** or 415-984-8409

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team