The Florida Bar Business Law Section Computer Law and Technology Committee Hot Topics

Labor Day Retreat 2017

1. Computer Fraud and Abuse Act – Narrowed in California federal district case (for now)
hiQ Labs, Inc. v. LinkedIn Corporation, Case No. 17-cv-03301-EMC (N.D Ca.)
hiQ's business involves providing information to businesses about their workforces based on statistician analysis of publicly available data. It initiated an action against LinkedIn after LinkedIn issued a cease and desist letter and attempted to terminate hiQ's ability to access otherwise publicly available information on profiles of LinkedIn users. The letter threatened actions under the Computer Fraud and Abuse Act (CFAA). LinkedIn also employed various blocking techniques designed to prevent hiQ's automated data collection methods. LinkedIN tolerated hiQ's access and use of its data for years.

   hiQ's complaint asserts affirmative rights against the denial of access to publicly available LinkedIn profiles based on California common law, the UCL, and the California Constitution. hiQ also seeks a declaration that hiQ has not and will not violate the CFAA, the DMCA, California Penal Code section 502(c), and the common law of trespass to chattels, by accessing LinkedIn public profiles. hiQ also filed a request for a temporary restraining order and an order to show cause why a preliminary injunction should not be issued against LinkedIn.

   On August 14, 2017, the court entered an order granting the motion for a preliminary injunction. The court found that in summary the balance of hardships "tips sharply" in hiQ's favor. The court stated that it is "doubtful that the Computer Fraud and Abuse Act may be invoked by LinkedIn to punish hiQ for accessing publicly available data; the broad interpretation of the CFAA advocated by LinkedIn, if adopted could profoundly impact open access to the Internet, a result that Congress could not have intended when it enacted the CFAA over three decades ago. Furthermore, hiQ has raised serious questions as to whether LinkedIn, in blocking hiQ's access to public data, possibly as a means of limiting competition, violates state law.

   The court deferred ruling on hiQ's argument that LinkedIn is violating antitrust law by denying it access to public data about its users. The court wrote, the "CFAA as interpreted by LinkedIn would not leave any room for the consideration of either a website owner's reasons for denying authorization or an individuals possible justification for ignoring such a denial."

   What did LinkedIn write in cease and desist letter?

   - Demanded that hiQ cease using software to "scrape," or automatically collect, data from LinkedIn's public profiles, noting that its User Agreement prohibits various methods of data collection from its website, and stating that hiQ was in violation of those provisions.
   - Stated that it had restricted hiQ's company page on LinkedIn, and that "any future access of any kind" to LinkedIn by hiQ would be "without permission and without authorization from LinkedIn."

- Stated that it had "implemented technical measures to prevent hiQ from accessing, and assisting others to access, LinkedIn's site, through systems that detect, monitor, and block scraping activity."
- Stated that any further access to LinkedIn's data would violate state and federal law, including California Penal Code section 502(c), the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. Section 1030, state common law of trespass, and the Digital Millenium Copyright Act.
- Reserved the right to pursue litigation, should hiQ fail to cease and desist from accessing LinkedIn's website, computer systems, and data.

2. Data Breach Victim Standing – Circuit Split Deepens
   Attias v. CareFirst, Inc., Case No. 16-7108 (D.C. Cir. Aug. 1, 2017)
   The D.C. Circuit ruled that alleged victims of a data breach have standing to pursue claims, notwithstanding that they have not yet suffered any actual harm as a result of the breach. This ruling adds to the prior circuit court rulings that have reached differing results when addressing the standing issue in data breach cases.

   Facts: Plaintiffs were the victims of an alleged data breach at health insurer CareFirst, which exposed their personal and medical data. Plaintiffs filed an 11-count class action raising state law claims in Maryland, Virginia and Washington, D.C. The District Court concluded that the plaintiffs lacked standing and granted a motion to dismiss based on a defense of lack of injury as a result of the breach. Since the plaintiffs' personal information had not yet been used to their detriment, and the complaint did not allege facts to support an inference that the PII was likely to be used in the future, the court dismissed the complaint on the basis of lack of standing.

   The D.C. Circuit reversed the dismissal, and concluded the opposite, that there was a high likelihood that the PII would be used in the future. The D.C. Circuit adopted the reasoning of the Seventh Circuit finding standing, asking "Why else would hackers break into a … database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

   The D.C. Circuit, in finding standing, joined the Third, Sixth, Seventh, and Eleventh Circuits in finding standing in a data breach case based solely on the likelihood of future harm. The Second and Fourth Circuits, on the other hand, have refused standing in data breach cases based on a risk of theft or misuse alone.

3. Podcasting "Patent Troll" Loses to EFF in Federal Circuit in "Save Podcasting" Campaign
   Personal Audio, LLC v. Electronic Frontier Foundation, Case No. 2016-1123 (Fed. Cir. Aug. 7, 2017)
   Facts: Personal Audio, LLC held what is essentially a podcasting patent entitled "System for Disseminating Media Content Representing Episodes in a Serialized Sequence," directed to a system and apparatus for storing and distributing episodic media files. The Patent Trial and Appeal Board in *inter partes* review, instituted on petition of the Electronic Frontier Foundation,

held the claims as unpatentable as anticipated under 35 U.S.C. Section 103, leading to the appeal.

The Federal Circuit affirmed the PTAB, and concluded that the challenged claims are anticipated by prior art, and, alternatively, that the claims are invalid as obvious in view of the prior art as well.

This case is the EFF’s Save Podcasting campaign.