Proskauer's Big Data - Small Breakfast for Large Hedge Fund Managers

August 7, 2018

Robert Leonard

Michael Mavrides

Jeffrey Neuburger

Joshua Newville

Christopher Wells

Proskauer

App Store T&C Update

- **App Store Review Guidelines former Section 5.1.2(ii)** (Emphasis added):
  - Data collected from apps may **not be used or shared** with third parties for purposes unrelated to improving the user experience or software/hardware performance connected to the app's functionality, or to serve advertising in compliance with the Apple Developer Program License Agreement.
- **As of June, 2018, the concept is subsumed into Section 5.1.2(i):**
  - Unless otherwise permitted by law, you may not use, transmit, or share someone's personal data without first obtaining their permission. You must provide access to information about how and where the data will be used. **Data collected from apps may only be shared with third parties** to improve the app or serve advertising (in compliance with the Apple Developer Program License Agreement.). Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program.
- **Unchanged (now in Section 5.1.2(ii) of App Store Review Guidelines**:
  - Data collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law.
- **Unchanged - Apple Developer Program Information**, Section 3.3.9: You and Your Applications … may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising … You may not use analytics software in Your Application to collect and send device data to a third party.

Scraping of “Public” Website Data

***hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F.Supp.3d 1099 (N.D. Cal. 2017)**

- Involves LinkedIn's challenge to hiQ's scraping of LinkedIn public profile data
- **Key question**: Whether, by continuing to access public LinkedIn profiles after LinkedIn explicitly revoked permission to do so, hiQ has "accessed a computer without authorization" within the meaning of the CFAA.
- Court granted injunctive relief against LinkedIn’s blocking of hiQ’s scraping activities.
- Lower court expressed "serious doubt" as to whether LinkedIn's revocation of permission to access the *public* portions of its site renders hiQ's access "without authorization."
  - “[I]n the context of a publicly viewable web page open to all on the Internet, the 'plainness' of the meaning of 'access' 'without authorization' is less obvious. Context matters.”
- **On appeal to the Ninth Circuit**. Oral arguments were held Mar. 15, 2018.

Scraping of "Public" Website Data

Sandvig v. Sessions, No. 16-1368 (D.D.C. Mar. 30, 2018)

- A group of professors and a media organization were conducting research into whether the use of algorithms by various housing and employment websites to automate decisions produces discriminatory effects
- Brought a constitutional challenge alleging that the potential threat of criminal prosecution under the CFAA for accessing a website "without authorization" violates their First Amendment rights.
- The court stated that much of the plaintiff's planned scraping behaviors – scraping of public website data, publishing of data stemming from such research and the use of bots to access and interact with a public website – were not CFAA violations.
- Scraping may be a violation of the ToS, but is not "exceeding authorized access."

Scraping of "Private" Websites

Ticketmaster L.L.C. v. Prestige Entm't, Inc., No. 17-07232 (C.D. Cal. Jan. 31, 2018)

- Defendant ticket brokers used bots and dummy accounts to navigate Ticketmaster's website and mobile app to purchase large quantities of tickets to popular events.
- As part of the ticket buying process, users must agree to Ticketmaster's terms of use before they can view and use Ticketmaster's website and mobile app.
- CFAA claim: Following *Power Ventures*, the court looked to the revocation of access and how it was communicated.
  - Ticketmaster contended that defendants lacked or exceeded their authorization by violating its terms, even after it sent defendants a cease and desist letter outlining the alleged violations.
  - In dismissing the claim, with leave to amend, the court found that Ticketmaster's cease and desist letter had "not shown that it rescinded permission from Defendants to use its website."
  - Court also noted that Ticketmaster's Complaint was "wholly devoid of any allegations suggesting that Ticketmaster took steps to prevent Defendants from future access."

Scraping of "Private" Websites

Ticketmaster L.L.C. v. Prestige Entm't, No. 17-07232 (C.D. Cal. May 29, 2018)

- Ticketmaster filed an (amended) complaint and defendant moved to dismiss.
- **CFAA**: Ticketmaster argued that each use of a bot to purchase a ticket was a use in excess of authorization because a C&D Letter explicitly prohibited defendants from using bots to access the site.
- Defendants countered that they did no more than violate the ToU, and as such cannot provide the basis for CFAA liability.
- Court allowed CFAA claim to go forward as it is the violation of the terms of the C&D Letter, not of Ticketmaster's terms, on which the court bases its finding of a well-pled CFAA claim.
  - "The *Power Ventures* court required something 'more' than mere violation of a website owner's terms of use to impose liability under the CFAA, and the Letter satisfies that requirement."

Scraping of “Private” Websites

***BidPrime, LLC v. SmartProcure, Inc.*, No. 18-478 (W.D. Tex. June 18, 2018)**

- Texas district court denied a bid from a web service for a TRO to enjoin a competitor that allegedly scraped a large amount of proprietary data from its closed site via several user accounts.
- While tempting to draw a general legal conclusion about the permissibility of scraping from this decision, the decision was in fact based on the judgement of the court that scraping was unlikely to continue during the pendency of the litigation.
- See also *Lemonade, Inc. v. One Versicherung AG*, No. 18-5368 (S.D.N.Y. Complaint filed June 14, 2018) (insurer lodged CFAA and contract claims against a competitor for allegedly created fake accounts to access the insurer’s app to extract data on pricing and claim procedures)

Scraping of "Private" Websites

Alan Ross Mach. Corp. v. Machinio Corp., No. 17-3569 (N.D. Ill. July 9, 2018)

- Plaintiff alleged its competitor Machinio Corp. scraped sales listings of industrial machines from plaintiff's website and listed such data on the Machinio site.
- Alan Ross alleged that it "expressly demanded that Machinio not scrape its website."
- Illinois district court dismissed claims, with leave to amend, relating to a competitor's alleged scraping of sales listings from a company's website for use on its own site.
- The court dismissed a CFAA claim that the defendant accessed the plaintiff's servers "without authorization," finding that the plaintiff failed to plead with specificity any damage or loss related to the scraping. In the court's view, the "mere copying of electronic information from a computer system is not enough to satisfy the CFAA's damage requirement."
- Court also dismissed plaintiff's breach of contract claims, concluding that defendant did not have notice of the plaintiff's website terms and conditions based upon an unenforceable browsewrap agreement.

MNPI – Deceptive Conduct

- DOJ – Use of SOX securities fraud statute 18 U.S.C. 1348
  - Section 1348 applied to insider trading (*e.g., U.S. v. Blaszczak*).
    (1) a scheme or artifice to defraud;
    (2) fraudulent intent; and
    (3) a nexus with a security.
  - Typical elements of 10b-5 insider trading are not applicable
    - No breach of fiduciary duty, personal benefit, or personal knowledge of the benefit.
- July 2018: *U.S. v. Korchevsky* criminal verdict
    - Mail fraud, wire fraud and securities fraud under Section 1348

MNPI – Deceptive Conduct

- SEC/Civil – 10b-5 “scheme” liability
  - *SEC v. Dubovoy*: hacking as a fraudulent device or scheme
    - Same scheme charged criminally in *Korchevsky.*
    - 2d Cir: misrepresenting ones identity in order to gain access is plainly “deceptive” under 10b-5
- Advisers Act Rule 204A
  - Failure to establish, maintain, and enforce policies and procedures reasonably designed to prevent the misuse of MNPI
  - Recent cases focus on inadequate measures to “enforce” policies and procedures, in light of particularized risks