FARELLA BRAUN + MARTEL LLP

JUNE 2021

Technology Ecosystems: Liability Arising from Relationships Between ISVs, API Developers, Scrapers, and Platforms

Stephanie Skaff & Alex Reese

This presentation is provided for informational purposes and does not constitute legal advice.

Discussion Topics

- Overview
  - Typical Platform Ecosystems: ISV “Partners,” API Developers, and Scrapers
  - Termination Can Take Many Forms
  - Representative Matters and Claims
- Platform Cases in the News
- Scraping and the CFAA: The Current State of Play
- Common Claims in Platform Ecosystem Disputes
- Antitrust/Unfair Competition Issues
- Tips

Overview

Typical Platform Ecosystems

Common Provisions in Independent Software Vendors (ISV) Agreements

- Money flows both ways (referral fees / commissions can be paid to either ISV or platform depending on where the end user originated).
- ISV may not compete directly with the platform.
- Platform may terminate for breach of platform governing rules.
- Term limited / must be renewed

Common Provisions in API Developer Agreements

- No payments.
- Either party may terminate at will, with or without cause.
- Developer may not compete directly with platform.
- Developer must abide by platform rules.

FARELLA BRAUN + MARTEL LLP

Termination Can Take Many Forms

Termination of ISV Contract

- Either refusal to renew or termination mid-contract

Economic Termination of ISV Contract

- Dramatic increase in price for continued platform access

Termination of API Developer Contract

- Most API agreements allow the platform to terminate at will and without cause

API Deprecation

- Technological termination; does not necessarily entail a change to any developer's contract

Assertion of CFAA or Terms of Use Against Scrapers

- Since there's no agreement in place, platforms rely on CFAA or Terms of Use to "terminate" scrapers

FARELLA BRAUN + MARTEL LLP

FBM Representative Matters in this Space

ISV Disputes

- Represented ISV in preparing complaint and TRO in anticipation of expected termination by Salesforce.

API Developer Disputes

- Represented API developer challenging Instagram's 2015 API deprecation. Prepared complaint and TRO; negotiated resolution.
- Represented platform in dispute with API developer that violated platform policies and was terminated; developer is asserting anticompetitive motivations.
- Represented platform alleging developers access to private API violated CFAA.

Scraper Disputes

- Represented hiQ in District Court and Ninth Circuit against LinkedIn.
- Provided counseling to scraper companies on CFAA, Terms of Use issues, and other claims
- Provided counseling to platform companies on enforcement under CFAA, tort and IP claims

FARELLA BRAUN + MARTEL LLP

Polling Question – Who's in the room?

Question: Does your company have relationships with independent software vendors, API developers, or has your company encountered issues with scraping?

Platform Termination Cases in the News

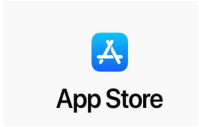
Epic Games v. Apple

- Maker of Fortnite claims that Apple abuses monopoly power.
- Market is defined as iOS app distribution market.
- Alleged violations include charging uncompetitive fees and restricting other distribution avenues.
- Trial concluded end of May.

FARELLA BRAUN + MARTEL LLP

Platform Termination Cases in the News

Apple App Store Class Actions



- Developer class action: *Cameron & Pure Sweat v. Apple*. Market is defined as iOS app and in-app purchase market. Hagens Berman appointed lead counsel.
- Consumer class action: *Pepper v. Apple*. Appealed to Supreme Court on *Illinois Brick* doctrine. SCOTUS held consumers had standing.

Google Play Store Class Action

- Consumer class action: *Carr v. Google*. Similar theory to *Pepper v. Apple*.

FARELLA BRAUN + MARTEL LLP

Scraping: The Current State of Play

FARELLA BRAUN + MARTEL LLP

Scraping Case Law – CFAA Developments

Van Buren v. United States, 19-783 (Sup. Ct. June 3, 2021)

- Police officer who used his credentials to access law enforcement database to obtain license information in exchange for money did not violate the "exceeds authorization" provision of the CFAA, even though his search violated the police department policy against obtaining database information for non-law-enforcement purposes.
- CFAA focuses on technical harm to computer system. Like the "without authorization" provision, the "exceeds authorized access" provision requires accessing a portion of a computer or computer system that the defendant had no authorization to access. A "gates up or gates down" analysis.
- Government's reading could criminalize innocuous employee conduct, and introduces arbitrariness by relying on how employers frame their internal policies.

FARELLA BRAUN + MARTEL LLP

Scraping Case Law – CFAA Developments

- *Van Buren* – companies can no longer pursue CFAA claims based on an employee or third party accessing for "improper purpose" – must show that access to the system or portion of the system was not authorized.
- *hiQ v. LinkedIn* – Supreme Court grants petition and remands in light of Van Buren.

  Cert. Issue: Whether a company that deploys computer "bots" to scrape data from public-facing websites—even after the website owner has expressly denied permission to access the data—"intentionally accesses a computer without authorization" in violation of the CFAA.

- Compare*: Facebook v. Power Ventures (9th)* – Power Ventures violated CCFA after permission to access was revoked by cease and desist letter; data gathered was protected by username/PW authentication

Scraping Case Law – CFAA Developments

- CFAA – open question: can companies use CFAA to prevent access to public data?
- Other Circuits:
  - *EF Cultural Travel* (1st) – finds liability for scraping public website in violation of terms of use
  - *Sandvig* (DC Dist. Ct.; ACLU challenge) – website terms of use cannot be basis for liability
  - *Drew* (CD Cal, cyberbullying case) – violation of terms of use too vague (criminal case)
- Other concerns:
  - Unconstitutional vagueness, *Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009); also noted by dissent in *Nosal I* and sometimes alternately objected to as improper "delegation"
  - "Information monopolies" not in public interest – *hiQ*
  - *Note* new EU legislation proposed – *DMA*

Claims by Platforms Against Scrapers

CFAA Claims

Knowingly “accessed” or accessed “beyond authorization” a protected computer for the purposes of obtaining information, causing damage, or perpetrating fraud.

18 U.S.C. §1030(a)(2), (a)(4), (a)(5).

Civil action requires a “loss”: Either (1) costs to investigate and respond, or *(2) costs associated with a service interruption.

CFAA – Scraper Responses

- Activity protected by the First Amendment
- Did not exceed “authorized” access because accessed by publicly-available means
- Did not “exceed” authorized access under Van Buren
- Customer/consumer information obtained is not “information” of the defendant
- Other defenses, including no “loss” of the type required by CFAA, SOL, etc.

Poll #2: Who's data is it anyway?

Question: If a platform end user gives their password and log-in to a third party for the purposes of scraping the user's data, does the third party violate the CFAA by scraping the user's data?

Contract “Terms of Use” Claims

Common fact pattern alleged :

- Platform’s “Terms of Use” prevent scraping, use of data by third parties

Common responses by scrapers:

- Terms of Use not enforceable contract
- Unclean hands/estoppel defenses
- Counterclaims

Other Claims Available to Platforms

- Trade Secret
  - *e.g.*, *Compulife v. Newman* (11th Cir. May 2020) (trade secret)
- Copyright
- Trademark
  - *e.g., Southwest v. Kiwi*
- Privacy-related claims
- Interference claims

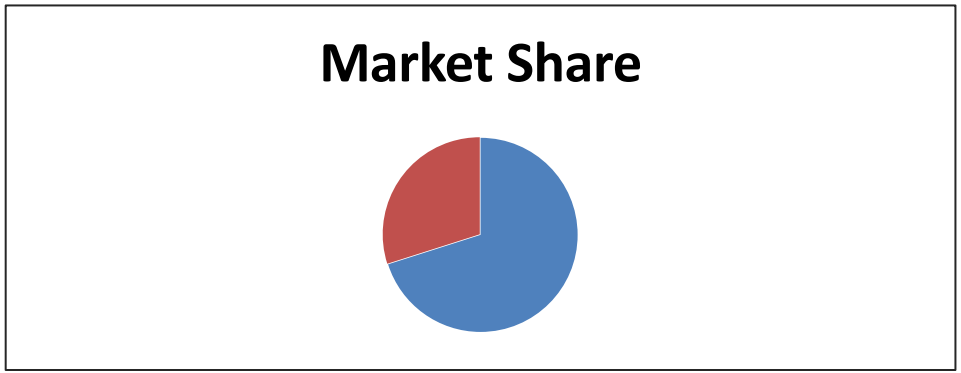
Potential Claims Against Platform if ISVs, API Developers, or Scrapers Are Terminated

Background Antitrust Norms

- No “duty to deal” except on mutually agreeable terms. *Verizon Commc’ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004)

Background Antitrust Norms

Very high market share threshold to establish market power (75% is a common rule of thumb, but at least 65% plus). *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 424 (2d Cir. 1945).



Antitrust & Unfair Competition Claims

How terminated parties attempt to overcome these background norms:

Essential facilities doctrine.

United States v. Terminal R.R. Ass'n, 224 U.S. 383 (1912);
Otter Tail Power Co. v. United States, 410 U.S. 366 (1973).

Lock-in theories.

Eastman Kodak Co. v. Image Technical Servs., Inc., 504 U.S. 451 (1992).

UCL sweeps more broadly

Cel-Tech Communications v. L.A. Cellular, 20 Cal. 4th 163, 186 (1999) (covers "incipient violations" of antitrust or violations of their "policy or spirit").

FARELLA BRAUN + MARTEL LLP

Antitrust & Unfair Competition Claims

Common fact pattern alleged in antitrust / unfair competition claims:

- Platform launched or is planning to launch a service competing with the terminated party.

- Platform acquired terminated party's competitor.

Tort Claims

- Breach of Contract
- Promissory Estoppel
- Interference Claims
- Other Tort Claims (Fraud, Trade Secret, Conversion)

Tort Claims

Common fact pattern alleged in promissory estoppel claims:

- Platform's public statements promoting an "open ecosystem."
- Platform's knowledge that developer built its business in reliance on continued access.

Interference Torts

Common fact pattern alleged in Interference Claims

- Platform's knowledge of developer's customers / contracts.
- Platform's cease and desist, notice of violation, or denial of access to its platform (usually by contract term changes, API deprecation / shutoff)
- Developer's inability to perform on its contracts or continue with its business
- Damages could include (1) lost business and bankruptcy or (2) non-monetary damages that might result in injunctive relief

Tips

Tips – If You're a Platform Restricting / Terminating Access

- Conduct an investigation into competing products / services under development to be prepared for antitrust / anti competition claims.
- If possible, terminate or restrict access on a party-neutral basis—don't target specific third parties, or specific kinds of services offered by third parties.
- Review press statements, contracts, and correspondence with third parties to identify potential reliance / promissory estoppel material they will rely on.
- Consider grace periods to reduce risk of TRO / PI motions.
- CFAA: Termination is strongest if the data is not publicly accessible and is owned by the platform (not its users)
- Terms of Use: Make sure Terms of Use are up-to-date and prohibit unauthorized use of platform data

FARELLA BRAUN + MARTEL LLP

Tips – If You're a Third Party Worried About Platform Termination

- Make clear to the platform your reliance on continued access.
- Identify public statements by the platform regarding continued access—e.g. "open ecosystem"
- Identify potential anticompetitive motives for the termination—competing products / services.
- Consider TRO / PI
  - Need evidence of irreparable harm. Destruction of business is usually sufficient. *See Am. Passage Media Corp. v. Cass Commc'ns, Inc.*, 750 F.2d 1470, 1474 (9th Cir. 1985).

Contact Information

Stephanie Skaff
sskaff@fbm.com

Alex Reese
areese@fbm.com

FARELLA BRAUN + MARTEL LLP