Proskauer's Big Data Breakfast

Robert Leonard
Michael Mavrides
Jeffrey Neuburger
Joshua Newville
Samuel Waldon
Christopher Wells

March 23, 2021

Proskauer

Agenda

- SEC Enforcement Update
- Updates on Apple/Android and Mobile App Data Collection
- Updates on the Fintech Privacy Litigations and Investigations
- Scraping & Data Harvesting Litigation Developments
- Relevant Legislative and Regulatory Developments
- APIs & Data Collection
- Final Thoughts

Biden Administration – SEC Enforcement Update

- On January 18, 2021, President Biden nominated Gary Gensler to serve as chairperson of the SEC:
  - Former head of the CFTC from 2009-2014
  - Participated in drafting the Sarbanes-Oxley Act as a senior adviser to former U.S. Senator Paul Sarbanes
  - On March 10, 2021, the Senate Banking Committee voted 14-10 to advance Gensler's nomination to the full Senate

- Generally, we expect to see a more aggressive approach to enforcement across the board:
  - Increase in enforcement actions against private funds
  - Focus on gatekeepers

- For big data:
  - We still expect that the SEC will issue guidance/risk alert before bringing actions
  - But the risk of enforcement actions has likely increased
  - Guidance is likely to come after appointment of senior staff (Exams, IM)

Mobile App Data

Apple and Mobile App Data

Recent changes to the App Store Requirements and what do they mean for the use of mobile-phone sourced alternative data?

Increased ambiguity

Apple and Mobile App Data

App Store Review Guideline updates now available

February 1, 2021

The App Store is a safe and trusted place for customers to discover and download apps, and a great opportunity for developers. The App Store Review Guideline changes and clarifications support new features in upcoming OS releases, better protect customers, and help your apps go through the review process as smoothly as possible. Review the

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). You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking. 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.

Apple and Mobile App Data

App Store Review Guideline updates now available

February 1, 2021

The App Store is a safe and trusted place for customers to discover and download apps, and a great opportunity for developers. The App Store Review Guideline changes and clarifications support new features in upcoming OS releases, better protect customers, and help your apps go through the review process as smoothly as possible. Review the

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).** You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking. 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.

Apple and Mobile App Data

App Store Review Guideline updates now available

February 1, 2021

The App Store is a safe and trusted place for customers to discover and download apps, and a great opportunity for developers. The App Store Review Guideline changes and clarifications support new features in upcoming OS releases, better protect customers, and help your apps go through the review process as smoothly as possible. Review the

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).** **You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking**. 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.

AP

Google ends sale of ads using individual web tracking data

GOOGLE ADS

Charting a course towards a more privacy-first web

David Temkin
Director of Product Management, Ads Privacy and Trust

Published 03 Mar 2021

Today, we're making explicit that once third-party cookies are phased out, we will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products.

Apple and Mobile App Data

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)**. You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking. 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.

What is "tracking"? Apple's definition:

"**Tracking**" refers to linking data collected from your app about a particular end-user or device, such as a user ID, device ID, or profile, with Third-Party Data for targeted advertising or advertising measurement purposes, or sharing data collected from your app about a particular end-user or device with a data broker.

Apple and Mobile App Data

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)**. You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking. 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.

What is "tracking"? Apple's definition:

"**Tracking**" refers to linking data collected from your app about a particular end-user or device, such as a user ID, device ID, or profile, with Third-Party Data for targeted advertising or advertising measurement purposes, **or sharing data collected from your app about a particular end-user or device with a data broker.**

Apple and Mobile App Data

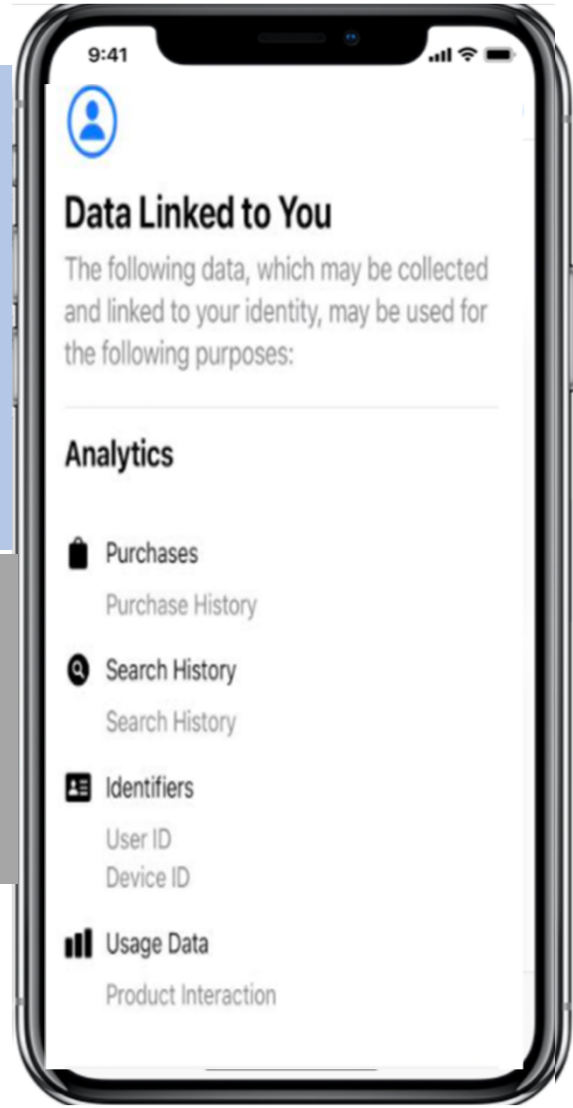
5.1.2(i) Unless otherwise permitted by law, you may not use, transmit, or share someone's personal data without first obtaining their permission. You must provide access to information about how and where the data will be used. **Data collected from apps may only be shared with third parties to improve the app or serve advertising (in compliance with the Apple Developer Program License Agreement)**. You must receive explicit permission from users via the App Tracking Transparency APIs to track their activity. Learn more about tracking. 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.

What is "tracking"? Apple's definition: "**Tracking**" refers to linking data collected from your app about a particular end-user or device, such as a user ID, device ID, or profile, with Third-Party Data for targeted advertising or advertising measurement purposes, **or sharing data collected from your app about a particular end-user or device with a data broker.**

If you use third-party code — such as advertising or analytics SDKs — you'll also need to describe what data the third-party code collects, how the data may be used, and whether the data is used to track users.

Does this mean that sharing with a data broker is OK as "tracking," even if not for purposes of improving the app or serving advertising?

Or can you only share with a data broker for improving the app or serving advertising?

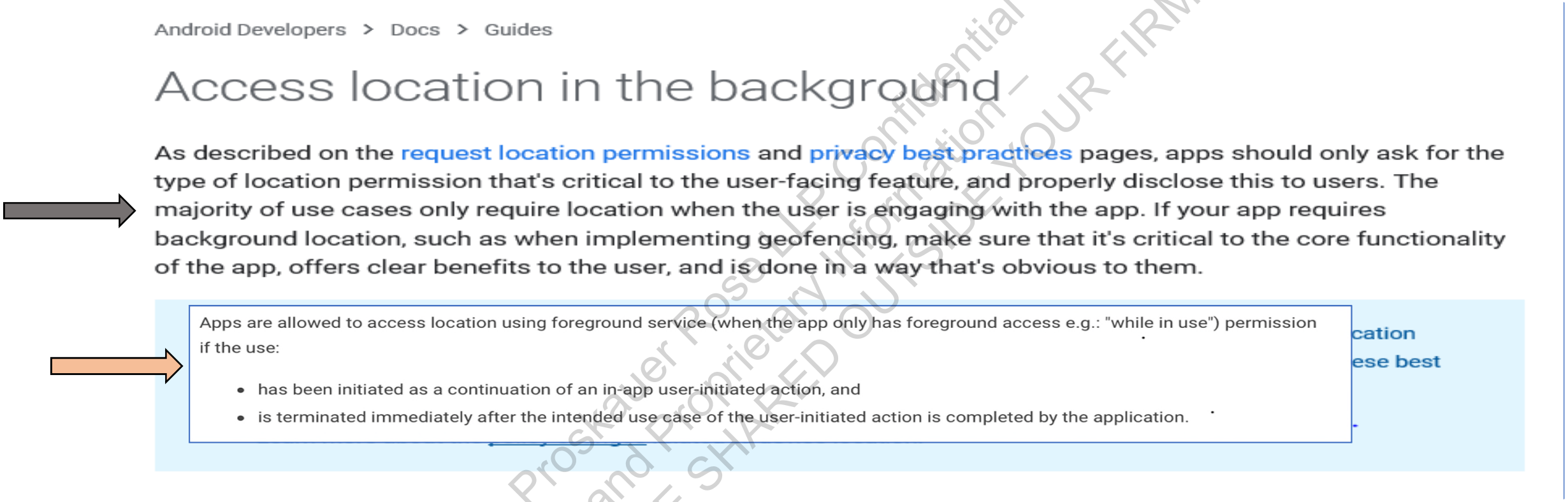


The Bottom Line with Apple

Recent changes to the App Store Requirements and what do they mean for the use of mobile-phone sourced alternative data?

- **Ambiguous as to sharing of data**
- **Concern**: Could the new disclosure requirement draw unwanted attention from regulators or private plaintiffs as to the accuracy of the disclosure?
  - Confusing requirements on disclosure – do providers understand the requirements?
  - Apps lack the ability to use nuanced privacy policy wording
  - Apple not verifying validity of disclosures
- **Recommendation**: If using iOS data (a risk-based analysis), new diligence and contract Items:
  - Are the app disclosures accurate and complete?
  - Contract representations re: accuracy
  - Notice of all investigations/lawsuits/complaints

Android-Based Locational Tracking



Android Developers > Docs > Guides

Access location in the background

As described on the request location permissions and privacy best practices pages, apps should only ask for the type of location permission that's critical to the user-facing feature, and properly disclose this to users. The majority of use cases only require location when the user is engaging with the app. If your app requires background location, such as when implementing geofencing, make sure that it's critical to the core functionality of the app, offers clear benefits to the user, and is done in a way that's obvious to them.

Apps are allowed to access location using foreground service (when the app only has foreground access e.g.: "while in use") permission if the use:

- has been initiated as a continuation of an in-app user-initiated action, and
- is terminated immediately after the intended use case of the user-initiated action is completed by the application.

cation
ese best

Beginning March 29, 2021, all existing apps (first published before April 16, 2020) that access location in the background will need to be approved or app updates may be blocked and your app may be removed from Google Play.

Diligence and Contract Items:

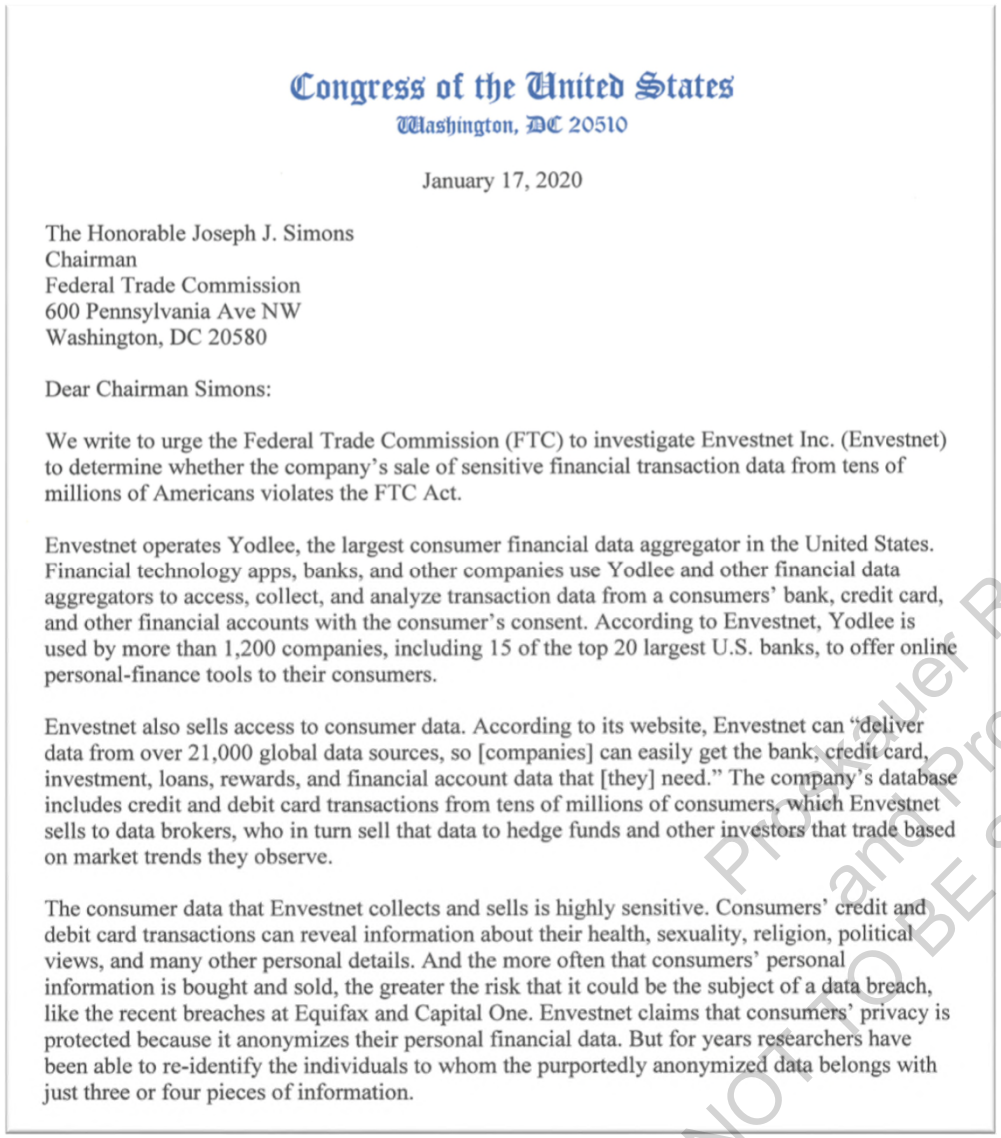
- **Foreground or background location collections?**
  - **Foreground: Appropriate Consents?**
  - **Background: Google approval?**

Litigation and Investigation Update

Update on *hiQ-LinkedIn*

- ***All quiet at the Supreme Court, cert. petition pending.***
- ***District Court Developments Continue:***
- Nov. 2020: Linkedin filed Counterclaims.
  - **Statement**: "Once data has been scraped, member data can end up in any number of databases controlled and used for any purpose. Data scraping therefore poses a significant threat to LinkedIn's business because it undermines the trust that LinkedIn has built with its members."
  - **CFAA**: robots.txt file, technical measures, security scans and places certain content behind password walls, thus, making hiQ's access "unauthorized" because "LinkedIn's website and servers are not unconditionally open to the general public."
  - **Breach of contract**: hiQ breached the user agreement that prohibit automated access
- Jan. 2021: hiQ files motion to strike counterclaims
  - **Statement**: "LinkedIn's counterclaims against hiQ are a transparent attempt by LinkedIn to pose as a defender of user privacy by characterizing hiQ as a "scraper" and a "free rider." […] Far from crusading for justice, LinkedIn is campaigning for its own bottom line and improperly attempting to use its counterclaims to shut down fair competition."
  - **CFAA**: Arguments already litigated; accessing publicly available data ≠ unauthorized access under the CFAA
  - **Breach of contract**: Even accepting that it might have breached the terms in the past, hiQ states it is no longer a user of LinkedIn and does not continue to breach the terms, thus negating any need for injunctive relief
  - **Trespass**: hiQ claims no harm has been shown
- Mar. 2021: Linkedin files opposition papers to hiQ's motion to strike the counterclaims

The Continuing Story of Yodlee…



Congress of the United States
Washington, DC 20510

January 17, 2020

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

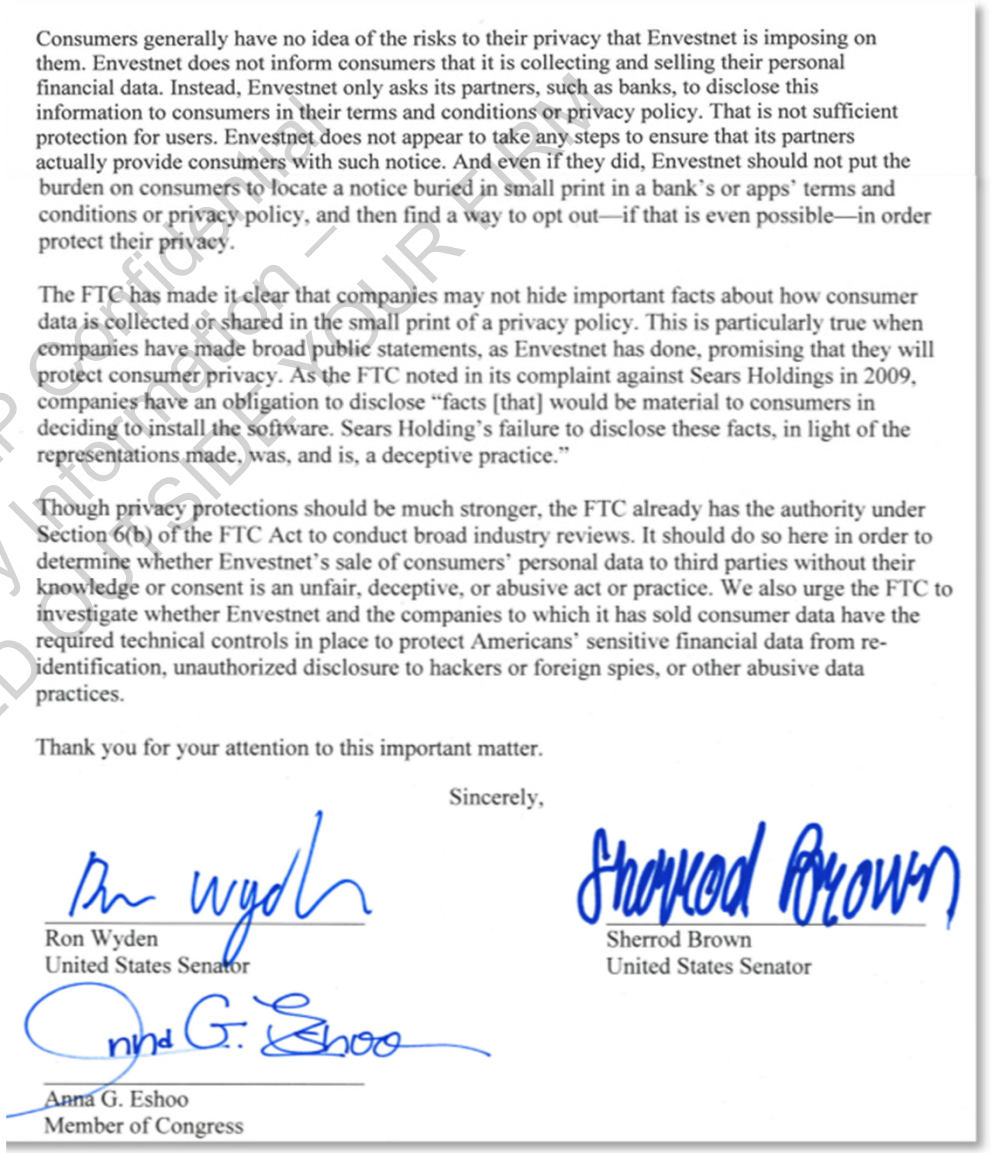
Dear Chairman Simons:

We write to urge the Federal Trade Commission (FTC) to investigate Envestnet Inc. (Envestnet) to determine whether the company's sale of sensitive financial transaction data from tens of millions of Americans violates the FTC Act.

Envestnet operates Yodlee, the largest consumer financial data aggregator in the United States. Financial technology apps, banks, and other companies use Yodlee and other financial data aggregators to access, collect, and analyze transaction data from a consumers' bank, credit card, and other financial accounts with the consumer's consent. According to Envestnet, Yodlee is used by more than 1,200 companies, including 15 of the top 20 largest U.S. banks, to offer online personal-finance tools to their consumers.

Envestnet also sells access to consumer data. According to its website, Envestnet can "deliver data from over 21,000 global data sources, so [companies] can easily get the bank, credit card, investment, loans, rewards, and financial account data that [they] need." The company's database includes credit and debit card transactions from tens of millions of consumers, which Envestnet sells to data brokers, who in turn sell that data to hedge funds and other investors that trade based on market trends they observe.

The consumer data that Envestnet collects and sells is highly sensitive. Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details. And the more often that consumers' personal information is bought and sold, the greater the risk that it could be the subject of a data breach, like the recent breaches at Equifax and Capital One. Envestnet claims that consumers' privacy is protected because it anonymizes their personal financial data. But for years researchers have been able to re-identify the individuals to whom the purportedly anonymized data belongs with just three or four pieces of information.



Consumers generally have no idea of the risks to their privacy that Envestnet is imposing on them. Envestnet does not inform consumers that it is collecting and selling their personal financial data. Instead, Envestnet only asks its partners, such as banks, to disclose this information to consumers in their terms and conditions or privacy policy. That is not sufficient protection for users. Envestnet does not appear to take any steps to ensure that its partners actually provide consumers with such notice. And even if they did, Envestnet should not put the burden on consumers to locate a notice buried in small print in a bank's or apps' terms and conditions or privacy policy, and then find a way to opt out—if that is even possible—in order protect their privacy.

The FTC has made it clear that companies may not hide important facts about how consumer data is collected or shared in the small print of a privacy policy. This is particularly true when companies have made broad public statements, as Envestnet has done, promising that they will protect consumer privacy. As the FTC noted in its complaint against Sears Holdings in 2009, companies have an obligation to disclose "facts [that] would be material to consumers in deciding to install the software. Sears Holding's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice."

Though privacy protections should be much stronger, the FTC already has the authority under Section 6(b) of the FTC Act to conduct broad industry reviews. It should do so here in order to determine whether Envestnet's sale of consumers' personal data to third parties without their knowledge or consent is an unfair, deceptive, or abusive act or practice. We also urge the FTC to investigate whether Envestnet and the companies to which it has sold consumer data have the required technical controls in place to protect Americans' sensitive financial data from re-identification, unauthorized disclosure to hackers or foreign spies, or other abusive data practices.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Sherrod Brown
United States Senator

Anna G. Eshoo
Member of Congress

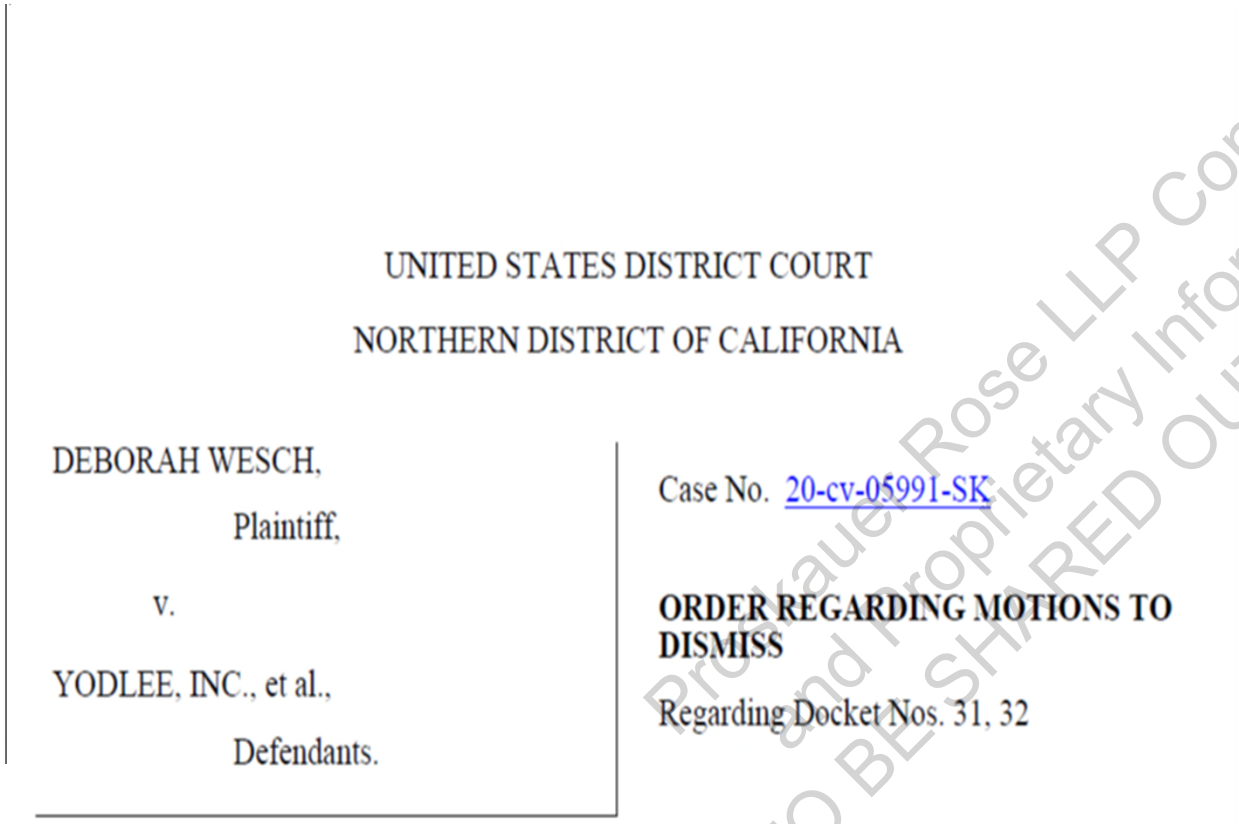
Envestnet 10-K, February 2020

"Recently, three members of Congress wrote to the Federal Trade Commission (the "FTC") to request a review of these business practices. In February 2020, we received a civil investigative demand from the FTC for documents and information relating to our data collection, assembly, evaluation, sharing, correction and deletion practices. We intend to cooperate with the FTC. If, as a result of the FTC's request, proceedings are initiated and we are found to have violated one or more applicable laws, we may be subject to monetary penalties and/or required to change one or more of our related business practices, any of which could have a material adverse effect on our results of operations, financial condition. Conduct giving rise to such liability could also form the basis for private civil litigation by third-parties allegedly harmed by such conduct."

Envestnet 10-K, February 2021

"Recently, three members of Congress wrote to the Federal Trade Commission (the "FTC") to request a review of these business practices. In February 2020, we received a civil investigative demand from the FTC for documents and information relating to our data collection, assembly, evaluation, sharing, correction and deletion practices, with which demand we fully complied. In November, 2020, we were informed by the FTC that it had closed the matter with no further action."

Class Action Filed August 25, 2020



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEBORAH WESCH,

Plaintiff,

v.

YODLEE, INC., et al.,

Defendants.

Case No. 20-cv-05991-SK

ORDER REGARDING MOTIONS TO DISMISS

Regarding Docket Nos. 31, 32

- Common Law Invasion of Privacy
- Federal Stored Communications Act
- Unjust Enrichment
- Acts of Deceit
- Unfair Competition
- California Comprehensive Data Access and Fraud Act
- Federal Declaratory Judgment Act
- California Anti-Phishing Act
- Computer Fraud and Abuse Act

Motion to Dismiss, Feb. 16, 2021

Yodlee Must Still Face Consumers' Privacy Suit

By *Emilie Ruscoe*

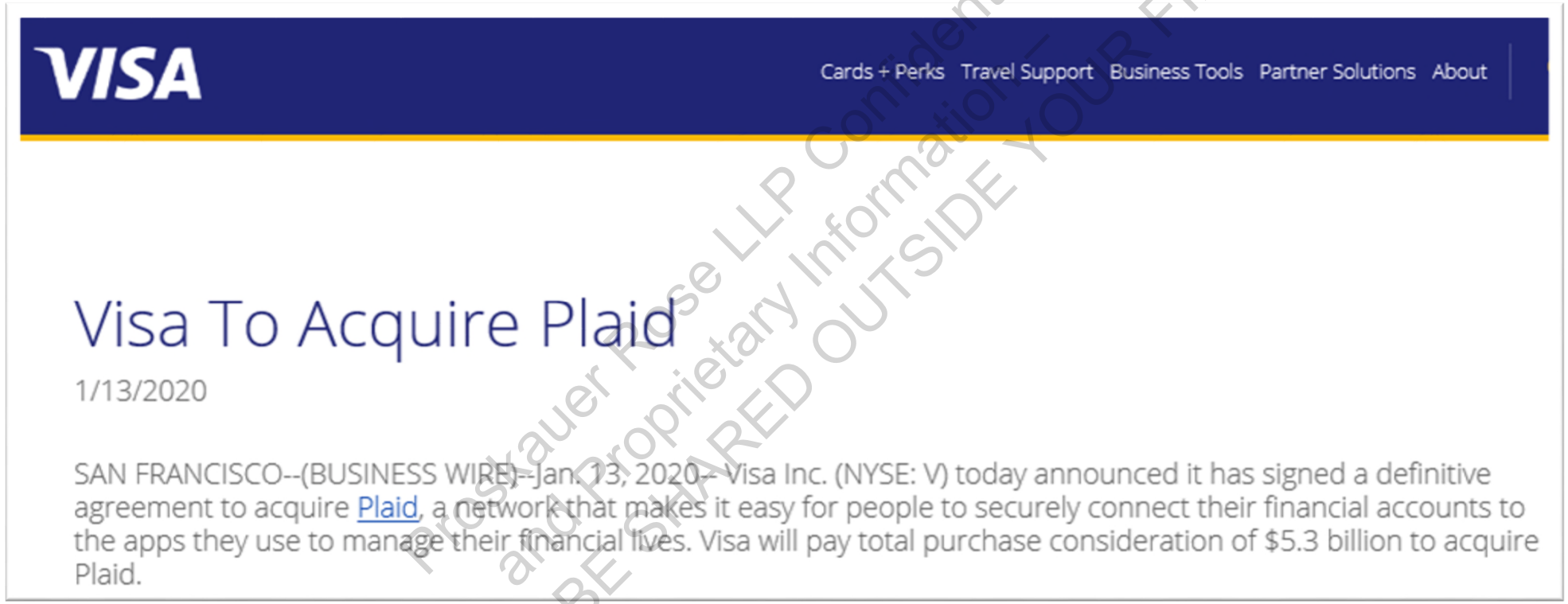
Law360 (February 17, 2021, 8:12 PM EST) -- Financial data aggregator Yodlee and its parent company Envestnet must continue to face consumer claims they secretly collected and sold users' highly sensitive banking data, a federal judge in San Francisco said.

In an order Tuesday, U.S. Magistrate Judge Sallie Kim left intact accusations of invasion of privacy, unjust enrichment, fraudulent deceit and violating California's Anti-Phishing Act of 2005 by Yodlee, siding with the users that they "have an expectation of privacy in their personal financial data, which Yodlee is collecting without their consent."

The judge dismissed claims brought under the federal Stored Communications Act and the Computer Fraud and Abuse Act and under California's Unfair Competition Law and Comprehensive Data Access and Fraud Act, but gave plaintiffs a chance to rewrite them.

- Common Law Invasion of Privacy
- ~~Federal Stored Communications Act~~
- Unjust Enrichment
- Acts of Deceit
- ~~Unfair Competition~~
- ~~California Comprehensive Data Access and Fraud Act~~
- Federal Declaratory Judgment Act
- California Anti-Phishing Act
- ~~Computer Fraud and Abuse Act~~

The Continuing Story of Plaid…



Antitrust Challenge Asserted

MARKETS | FINANCE

Justice Department Files Antitrust Lawsuit Challenging Visa's Planned Acquisition of Plaid

DOJ says acquisition would allow Visa to unlawfully maintain a monopoly in online debit market

JOHN R. READ (DC Bar #419373)
MEAGAN K. BELLSHAW (CA Bar #257875)
CORY BRADER LEUCHTEN (NY Bar # 5118732)
SARAH H. LICHT (DC Bar #1021541)
United States Department of Justice, Antitrust Division
450 Fifth Street, NW, Suite 4000
Washington, DC 20530
Telephone: (202) 307-0468
Facsimile: (202) 514-7308
E-mail: john.read@usdoj.gov

[Additional counsel listed on signature page]

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, *Plaintiff* v. VISA INC. and PLAID INC.,	Case No.: **COMPLAINT**

Forbes

BREAKING | Jan 12, 2021, 05:22pm EST | 5,739 views

Visa, Fintech Startup Plaid Drop Merger Plans After DOJ Antitrust Lawsuit

Rachel Sandler Forbes Staff

Business

I cover breaking news.

Updated Jan 13, 2021, 11:59am EST

TOPLINE Visa and fintech startup Plaid ditched plans for a $5.3 billion merger Tuesday after a Department of Justice antitrust lawsuit had threatened to block the deal.

At Least Five Class Actions Against Plaid

Actions Consolidated in July 2020 (*In re Plaid Inc. Privacy Litig.*)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JAMES COTTLE and FREDERICK SCHOENEMAN, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

PLAID INC., a Delaware corporation,

Defendant.

Case No.: _____

COMPLAINT FOR DAMAGES AND DECLARATORY AND EQUITABLE RELIEF

CLASS ACTION

Feb. 2021: Hearing held on Plaid's motion to dismiss; matter taken under submission.

attention."[43] In August 2018, a programmer who formerly worked for Plaid confirmed that the company "perform[ed] huge amounts of analytics on customer data acquired as part of the account verification process." The programmer also highlighted the economic value of the analytics Plaid performs on the banking data, explaining how the data may be monetized by selling the "derivative analytics" of the data to hedge funds, who use the analytics to forecast the revenue of companies in advance of equity earnings announcements.[44]

54. As Perret explained in May 2019, Plaid's long-term business plan is to monetize

TD Brings Action Against Plaid

Case 1:20-cv-14424-RMB-JS Document 1 Filed 10/14/20 Page 1 of 20 PageID: 1

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

THE TORONTO-DOMINION BANK,

Plaintiff,

v.

PLAID INC.,

Defendant.

Civil Action No. ____

Document Electronically Filed

COMPLAINT FOR TRADEMARK COUNTERFEITING, TRADEMARK INFRINGEMENT, FALSE DESIGNATION OF ORIGIN

4. TD brings this action because Defendant Plaid Inc. has created a user interface ("UI") for financial services applications that uses TD's TD and TD BANK trademarks, logo, and green color scheme to replicate TD's genuine login page and to dupe consumers into believing they are entering their sensitive personal and financial information in the bank's trusted and secure platform. ***In reality, however, consumers are unwittingly giving their login credentials to Defendant, who takes the information, stores it on its servers, and uses it to mine consumers' bank records for valuable data (e.g., transaction histories, loans, etc.), which Defendant monetizes by selling to third parties.*** Defendant's unscrupulous practices are the subject of a separate consumer class action for invasion of privacy and other wrongs.

Feb. 2021: Plaid given extension to file Answer to complaint.

BrandTotal Browser Extension Scraping The Case Continues…

DigitalNewsDaily

Facebook Battles BrandTotal Over Data Scraping

by **Wendy Davis** **@wendyndavis**, October 22, 2020

Get paid for the time you spend online doing the things you love to do.

Facebook alleges:

1. Defendants' extensions were programmed to send commands to Facebook and Instagram servers appearing to originate from the user.
2. Browser extensions harvested, without Facebook's authorization, behind the firewall information including users' profile information, user advertisement interest information and various ad metrics when the users visited Facebook, Instagram or various other social sites (all despite users' account privacy settings).
3. The data collected by defendants was then presumably used to provide "marketing intelligence" services about users and advertisers.

BrandTotal Browser Extension Scraping The Case Continues…

- ***Facebook Inc. v. BrandTotal Ltd.*, No. 20-07182 (N.D. Cal. Feb. 19, 2021)**

"With the contractual provision that Facebook sought to enforce apparent from the face of BrandTotal's counterclaim and no allegation of bad faith, BrandTotal's counterclaim for interference with contract is DISMISSED based on Facebook's legitimate business purpose…."

Facebook Gets Ad Firm's Claims Tossed In Data Scraping Row

By Christopher Cole

Law360 (February 23, 2021, 5:34 PM EST) -- A California federal magistrate judge tossed multiple claims that Facebook unlawfully blocked an ad firm's data-scraping tool, but said most of the allegations can be refiled if gaps in the claims are fixed.

Israeli luxury advertising firm BrandTotal is fighting Facebook in a Silicon Valley court case originally brought by the social media company to prevent the ad firm from harvesting user data from the platform. BrandTotal says the information gathered is "innocuous" and not sensitive, but that Facebook has sought to monopolize the data.

More Facebook Suits over Browser Extensions

Facebook sues two Chrome extension devs for scraping user data

Facebook filed a lawsuit today in Portugal against browser extension maker Oink and Stuff.

"When people installed these extensions on their browsers, they were installing concealed code designed to scrape their information from the Facebook website, but also information from the users' browsers unrelated to Facebook — all without their knowledge," Jessica Romero, Facebook's Director of Platform Enforcement and Litigation, said today.

"If the user visited the Facebook website, the browser extensions were programmed to scrape their name, user ID, gender, relationship status, age group and other information related to their account," Romero said.

By Catalin Cimpanu for Zero Day | January 14, 2021 -- 20:16 GMT (12:16 PST) | Topic: Security

Screen Scraping

Southwest Airlines Sues to Stop Web Scraping of Fare Information

Thursday, January 21, 2021

On January 14, 2021, Southwest Airlines Co. ("Southwest") filed a complaint in a Texas district court against an online travel site, Kiwi.com, Inc. ("Kiwi"), alleging, among other things, that Kiwi's scraping of fare information from Southwest's website constituted a breach of contract and a violation of the Computer Fraud and Abuse Act (CFAA). (*Southwest Airlines Co. v. Kiwi.com, Inc.*, No. 21-00098 (N.D. Tex. filed Jan. 14, 2021)). Southwest is no stranger in seeking and, in most cases, obtaining injunctive relief against businesses that have harvested

- Complaint alleges trademark violations (Lanham Act, etc.), breach of contract, violations of the CFAA (and Texas state computer trespass law), unjust enrichment and other claims.
- The case involves a "browsewrap" agreement but the defendant had notice of the terms from a C&D letter.
- Does hiQ apply? Is the data "public" data?
- Motions to Dismiss pending; Southwest's motion for a Preliminary Injunction barring Kiwi's sales of Southwest flights pending.

Screen Scraping
Question from a client:

- When a vendor uses a proxy to web scrape – should the website operator be able to determine a vendor's identity behind the proxy server IP address or is it enough for the operator to see the proxy's IP only?
- Does it matter the intent behind the use of the proxy? For example, to access web content in other countries where there might be geographical limitations vs. intentionally masking/obfuscating the IP address?

Update: Google Still Facing Handful of Data Collection Suits

DigitalNewsDaily

Judge Refuses To Dismiss Arizona Suit Against Google Over Location Privacy

by **Wendy Davis** **@wendyndavis**, October 8, 2020

Arizona's top law enforcement official can proceed with a lawsuit accusing Google of misleading the public about location privacy, a state judge has ruled.

The decision, issued by Maricopa County Superior Court Judge Timothy Thomason, comes in a lawsuit brought earlier this year by state Attorney General Mark Brnovich, who alleged that Google engaged in the "widespread and systemic use of deceptive and unfair business practices to obtain information about the location of its users" for ad purposes.

A class of individuals, whose mobile app usage was tracked by Google despite turning off "Web & App Activity" tracking, filed a complaint on Tuesday in the Northern District of California against Google and its parent company Alphabet Inc. for the unlawful interception and surreptitious collection of their communications and data.

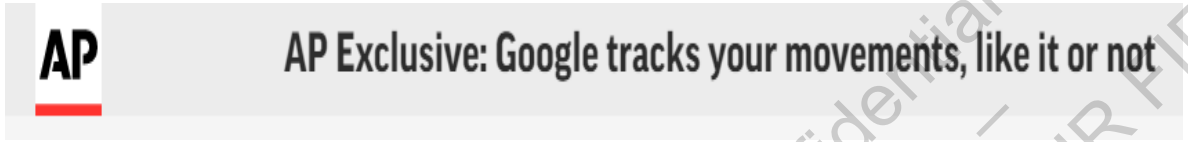
Docket Alarm Alerts Ce

Click the links below to see other recen
involving the parties, judges, and law fi
in this Law Street story. Press "Track S

Dec. 2020: State's partial summary judgment motion fully submitted re: state consumer protection claims related to a subset of legacy Android phones.
Case remains ongoing.

March 2021: Hearing held re: Google's motion to dismiss amended complaint, arguing apps with Firebase SDK consented to data collection and had given notice to users. Decision pending.

In re Google Location History Litig., No. 18-05062 (N.D. Cal. Jan. 25, 2021)


AP Exclusive: Google tracks your movements, like it or not


Facebook, Google Hit With Suits Over Location Tracking

By Allison Grande

Law360 (October 22, 2018, 10:49 PM EDT) -- Facebook and Google surreptitiously track, log and store users' private location information, even in circumstances where consumers explicitly limit or turn off this data collection capability, according to separate putative class actions lodged in California federal court Friday.

In one of the new complaints, Facebook user Brett Heeger claims the social media giant misleads users by offering them the option to restrict it from gathering and storing their location data, when in reality the company continues to scoop up this information and feeds it into a "Location History" feature that can build a history of precise locations used for targeted advertising.

Plaintiffs: Google erroneously told users they could "turn off Location History at any time" and that, with Location History off, "the places you go are no longer stored," but, in reality, the Web & App Activity setting is different and is "on" by default and saves certain information about a user's "activity on Google sites and apps to give you faster searches…[etc.]"

- **Jan. 2021**: District court dismissed some claims, allowed others.
  - The court allowed common law privacy claims, finding that Plaintiffs' allegations that Google collected and stored comprehensive location data without Plaintiffs' consent are sufficient to show that Plaintiffs had a reasonable expectation of privacy in the sum of that data.

McCoy v. Alphabet, Inc., No. 20-05427 (N.D. Cal. Feb. 2, 2021)

Google's Consent Defense Can't Ax Data Privacy Suit Outright

By Dorothy Atkins

Law360 (February 3, 2021, 6:07 PM EST) -- A California magistrate judge on Tuesday trimmed claims from an Android smartphone user's proposed class action alleging Google illegally harvests third-party app data to gain an advantage over rivals like TikTok, but she rejected Google's argument that users clearly agreed to the data collection by accepting its privacy policy.

In a 25-page decision, U.S. Magistrate Judge Susan van Keulen said the privacy policy at issue in this case isn't as specific as the policy at issue in the Smith v. Facebook Inc. case, which a district judge dismissed in 2017 after he found the plaintiffs consented to Facebook's tracking activities.

- Various privacy claims relating to Google's alleged inadequate notice of and alleged use of internal program "Android Lockbox" to collect sensitive PI related to third party app usage on Android phones.
  - *Claims*: common law/state privacy claims, deceit, CCPA, consumer claims, breach of contract, unjust enrichment
- **Consent inadequate** Privacy Policy example ("We collect information about your activity in our services [including] Activity on third-party sites and apps that use our services")
  - Court: Privacy policy lacks specificity, such language "may not be understood by a reasonable user to include data from apps that are not associated with Defendant's services."
  - "Disclosure and acceptance of statements for a different purpose is not sufficient to establish explicit consent to the collection of information regarding use of third-party-apps for the purposes of using that information to Defendant's competitive advantage."
- **Yet**, the court dismissed common law privacy claims as plaintiff failed to plead that the anonymized, aggregated app usage data was an "egregious" breach or intrusion required for a cognizable claim.

Google Can Be Sued for Tracking Users in Private Browsing Mode, Judge Says

Jody Serrano
Today 3:02PM

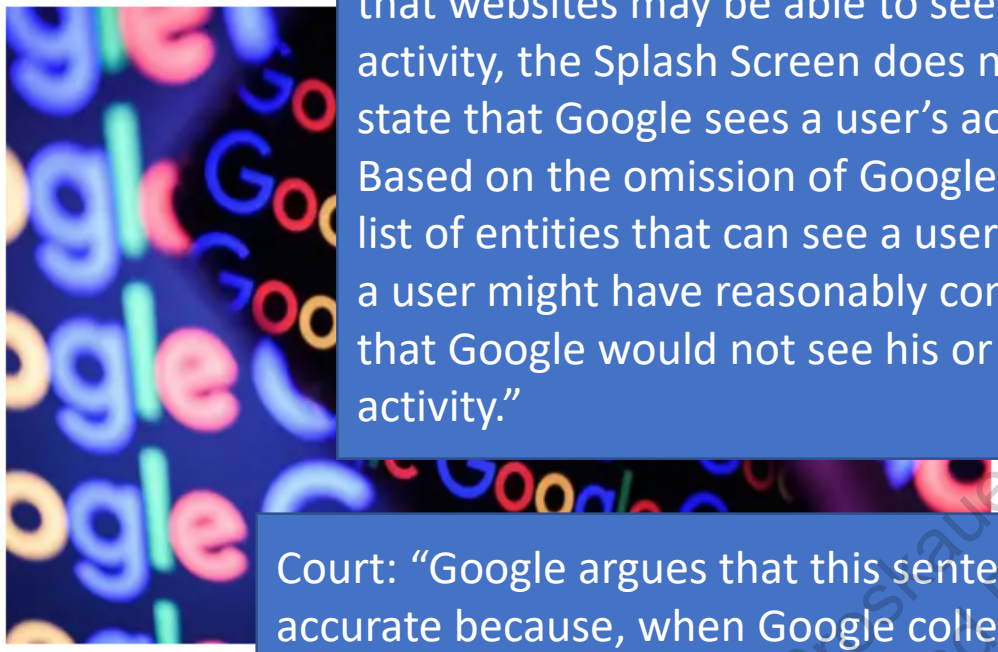


Photo: Leon Neal (Getty Images)

A U.S. district j
collecting data
selected browse

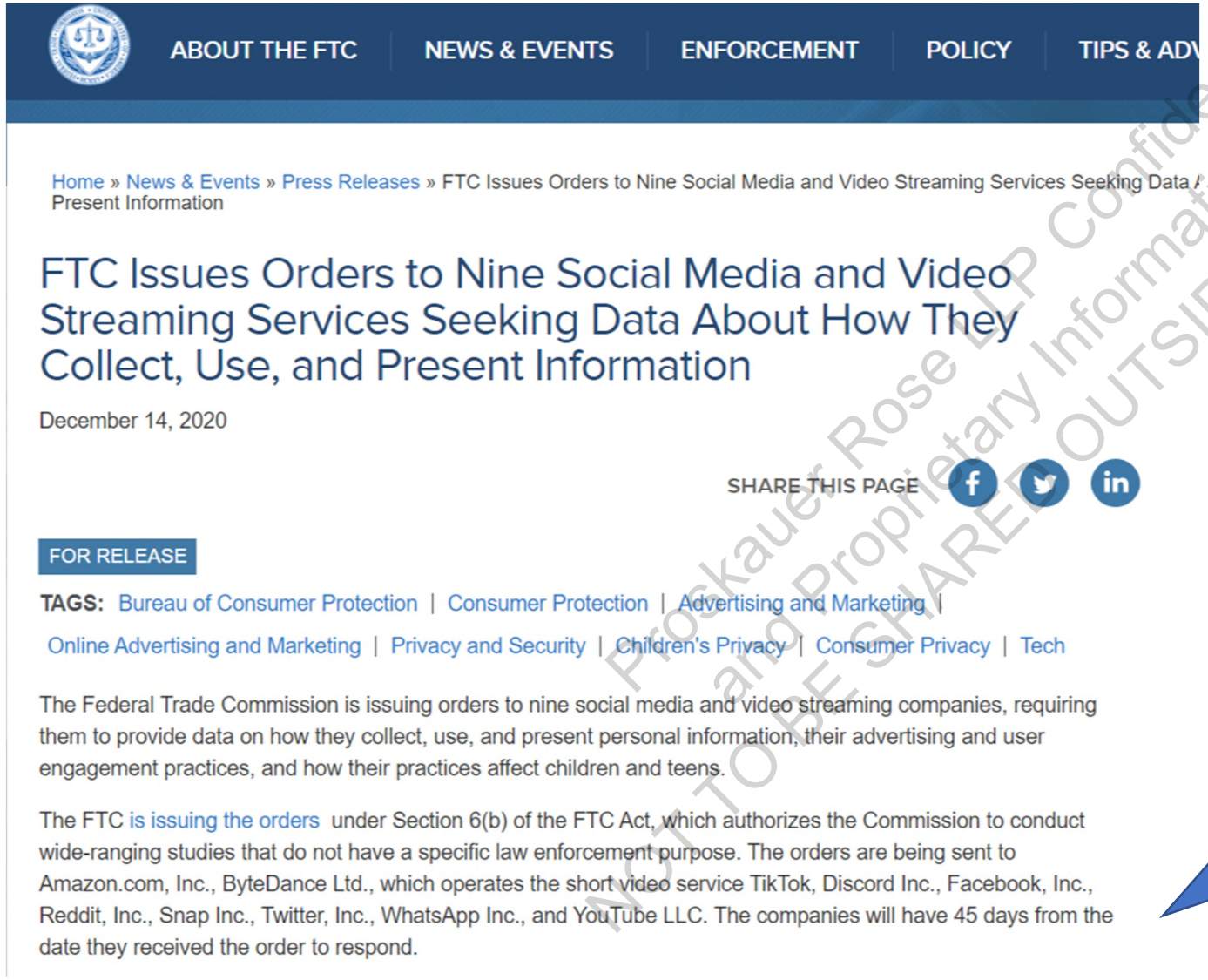
March 12, 2021

Court: "Although the Splash Screen states that websites may be able to see a user's activity, the Splash Screen does not state that Google sees a user's activity. Based on the omission of Google from the list of entities that can see a user's activity, a user might have reasonably concluded that Google would not see his or her activity."

Court: "Google argues that this sentence is accurate because, when Google collects the alleged data, Chrome is not storing the data; rather, the user's browser is transmitting the data to Google's server. However, the Court concludes that a reasonable user could read this statement to mean that their browsing history and cookies and site data would not be saved."

Legislative and Regulatory Developments

FTC Investigation (Section 6(b)) of Data Sharing by Social Media Applications



ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADV

Home » News & Events » Press Releases » FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Present Information

FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information

December 14, 2020

SHARE THIS PAGE

FOR RELEASE

TAGS: Bureau of Consumer Protection | Consumer Protection | Advertising and Marketing | Online Advertising and Marketing | Privacy and Security | Children's Privacy | Consumer Privacy | Tech

The Federal Trade Commission is issuing orders to nine social media and video streaming companies, requiring them to provide data on how they collect, use, and present personal information, their advertising and user engagement practices, and how their practices affect children and teens.

The FTC is issuing the orders under Section 6(b) of the FTC Act, which authorizes the Commission to conduct wide-ranging studies that do not have a specific law enforcement purpose. The orders are being sent to Amazon.com, Inc., ByteDance Ltd., which operates the short video service TikTok, Discord Inc., Facebook, Inc., Reddit, Inc., Snap Inc., Twitter, Inc., WhatsApp Inc., and YouTube LLC. The companies will have 45 days from the date they received the order to respond.

Includes: **Amazon, ByteDance (Tik Tok), Discord, Facebook, Reddit, Snap, Twitter, WhatsApp and YouTube**

New York State
Department of Financial Services

Report on Investigation of Facebook Inc. Data Privacy Concerns

February 18, 2021

NYS DFS Facebook Investigation

Facebook offers app developers who download Facebook's Software Development Kit ("SDK") access to free online data analytics services…. [It] allows app developers to integrate Facebook with their app by automatically transmitting data from the mobile app or website to Facebook so that the data can be analyzed. [Information includes a device's IP address and type, the time of use, and a device's advertising ID and information about] opening the app, clicking, swiping, viewing certain pages, placing items into a checkout, and so on.

NYS DFS Facebook Investigation

The information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data.

NYS DFS Facebook Investigation

These recommendations are not limited to Facebook, as it appears that the problematic data-sharing practices exposed in the WSJ Article are a continuing risk throughout the data analytics and social media industries. All companies within that industry — as well as the relevant regulatory bodies with oversight over those companies — should proactively take all reasonable steps to eliminate the practice of unauthorized sharing of sensitive user data with third-parties, whether they are business partners, advertisers or otherwise.

NYS DFS Facebook Investigation

This troubling lack of privacy protection at Facebook illustrates a larger problem with the data analytics industry. The way Facebook receives and uses data from third parties is not unique to Facebook, and the issues identified in the WSJ Article are present to some extent throughout the data analytics industry. The problems uncovered in this Report clearly show that there is a need for more transparency and public oversight of the "big data" industry.

Our regulatory institutions need to rapidly adapt to the challenges presented by social media giants, big tech, and the analytics industry, and it is imperative that we put in place a clear nationwide legal framework for accountability enforced by a robust federal regulator.

State Privacy Laws

Virginia governor signs comprehensive data privacy law

BY REBECCA KLAR - 03/02/21 05:24 PM EST

- **Like the CCPA…** the VCDPA (which goes into effect on Jan. 1, 2023) generally grants consumers various rights re: data access, correction, deletion and the right to opt-out of the "sale" of PI (though the definition is narrower than the CCPA), including the right of opt-out of the "processing" of personal data for targeted advertising.
- **Like the CPRA…** the VCDPA also governs "sensitive" information and allows consumers to places limits on the sale, sharing and use of sensitive information. The CPRA offers some opt-out rights for data processing, while the VCDPA requires the data controller to obtain the consumer's consent before processing sensitive information.
- **Sensitive data under the VCDPA**: "1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or **4. Precise geolocation data**."

JANUARY 15, 2021 | Albany, NY

Governor Cuomo Announces Proposal to Safeguard Data Security Rights as Part of the 2021 State of the State

2021 STATE OF THE STATE

STATE

Florida officials weigh major data privacy legislation

Governor Cuomo Announces Proposal to Safeguard Data Security Rights as Part of the 2021 State of the State

Washington State Takes Another Run at Online Privacy Rules

With the backing of big technology companies like Amazon and Microsoft, the Washington Privacy Act could mean new rights for the consumer. But not everyone is convinced the bill has the teeth it needs to work.

nounced a comprehensive law that will provide New Yorkers eir personal data and provide new privacy protections as part will mandate that companies that collect information on disclose the purposes of any data collection and collect only data needed for those purposes. Governor Cuomo will also establish a Consumer Data Privacy Bill of Rights guaranteeing every New Yorker the right to access, control, and erase the data collected from them; the right to nondiscrimination from providers for exercising these rights; and the right to equal access to services.

ISP Privacy

President Biden's FCC appointment is a big step toward net neutrality's return

Opinion: Jessica Rosenworcel, who's been pro-net neutrality for years, has been named the Federal Communications Commission's acting chairwoman.

New FCC net neutrality order could again include privacy/data collection restrictions.
Reports suggest a net neutrality bill will also be introduced in Congress soon.

Maine Fends Off Challenge Against Internet Privacy Law

By *Khorri Atkinson*

Law360 (July 7, 2020, 9:31 PM EDT) -- Maine notched a significant victory Tuesday after a federal judge rejected internet service providers' bid to overturn the state's new landmark online privacy statute on First Amendment grounds and ruled that the law limiting the use of customers' personal data is not preempted by federal law.

U.S. District Court Judge Lance Walker, who examined the parties' dueling requests for a judgment on the pleadings, struck down a key argument asserted by the ISP challengers – that the statute conflicts with existing federal law. The statute prohibits internet service providers from using or selling consumer browsing history and other data without first obtaining consent.

35-A M.R.S. §9301 which took effect in July 2020, prohibits, with some exceptions, Maine broadband providers from using, disclosing, selling or permitting access to customer's PI unless the customer expressly consents. It also allows a customer to opt out of other collection of non-PI.

PI includes: browsing/app use history, precise location data, financial info, etc.

Feb. 2020: Trade groups challenged the law on federal preemption and constitutional grounds.

July 2020: Court struck down First Amendment and preemption arguments. Case remains ongoing.

APIs and Data Collection

API Enforcement

Twitter Cuts Off Popular Third-Party Management Tools Due to API Violations

AUTHOR

Andrew Hutchinson

@adhutchinson

PUBLISHED

Feb. 1, 2019

If you log onto your favorite Twitter management app today, you may be in for a surprise.

This week, Twitter has enforced tighter restrictions on its API use in order to limit the capacity of tools which allow "bulk and aggressive" following behavior, like following and unfollowing many accounts at once. Tools

ZDNet

VIDEOS WINDOWS 10 5G BEST VPNS CLOUD SECURITY AI MORE NEWSLETTERS ALL WRITERS

MUST READ: Microsoft Exchange Server hacks 'doubling' every two hours

Twitter says an attacker used its API to match usernames to phone numbers

Twitter discloses security incident involving the abuse of one of its official API features.

Twitter cracks down on API abuse, will charge B2B devs

Josh Constine @joshconstine / 1:01 PM EDT • March 19, 2019

Comment

Reddit APIs

r/redditdev · Posted by u/johanneak 1 month ago

Wallsteeetbets APIs

Reddit API

Hi! I'm writing a bachelor thesis on Gamestock. I would have to do a document analysis and retrieve info on r/wallstreetbets. For me to get as much info as possible, I will have to cover the most essential information regarding this specific thread. I need statistics on who posts there, what words are used, what type of posts..

How should I proceed? What type of APIs do I need, or best suits my purpose? I have been in contact with admins of reddit, they suggested that I contacted the mods, but they have yet to respond. BTW I'm using RStudio.

busymichael 1 month ago

I have been running data analysis on r/wallstreetbets for many years using the reddit public api and python scripts. The other comments in this thread will get you started.

One note: you will not be able to get much older information from the public api. Look at pushshift.io as a way to access older posts.

Edit: I guess pushshift.io has been down for a few days (apparently many people have had similar ideas of using it to get info out of wsb). It is still the best source for older data, though, so just try it again in a week.

2 Reply Share Report Save

Reddit API Terms

Reddit API Terms of Use

API Terms of Use
Effective Date: May 25, 2016

Thanks for inquiring al
data, code, and other r
Collectively, we refer t
accompanying API doc
"Terms." By using the
disagree with any of th
APIs.

1. Registration.

a. Accepting the Term
(a) you are not of legal
person barred from us
United States or other
which you use the Red

b. Corporate Use. If y
entity, you represent ar
or the applicable entity
you agree, on behalf o
authority to bind your

Search

Reddit API Access

We want to allow developers to build great products powered by Reddit and we recognize developer community is integral to the success of the Reddit platform. We also want prote users' privacy and security regardless of how they choose to consume Reddit content.

In order to access the Reddit API directly, please make sure you comply with the following

- **You must read the terms and register in order to use the Reddit API**
- All API clients must authenticate with OAUTH 2
- All API clients must follow the API rules: https://github.com/reddit/reddit/wiki/API
- You may not use the Reddit logos and trademark without ap
- You may use "for reddit" or "a client for reddit" in the title of t use "reddit" without "for" preceding it. You may not use the word e, keyw description in any way that implies the app was developed by Reddit, Inc.
- If your intended usage is commercial, you'll need approval from us (either by filling out terms form or emailing api@reddit.com. Use of the API is considered "commercial" if y earning money from it, including, but not limited to in-app advertising, in-app purchas you intend to learn from the data and repackage for sale. Open source use is generally considered non-commercial.

Read the full API terms and sign up for usage.

What exactly is "commercial" use of the API?

Reddit API

I'm just a 🦍 who follows r/wallstreetbets. I want to write a script to figure out what trades they're making. On https://www.reddit.com/wiki/api:

> If your intended usage is commercial, you'll need approval from us (either by filling out the API terms form or emailing api@reddit.com. Use of the API is considered "commercial" if you are earning money from it, including, but not limited to in-app advertising, in-app purchases or you intend to learn from the data and repackage for sale. Open source use is generally considered non-commercial.

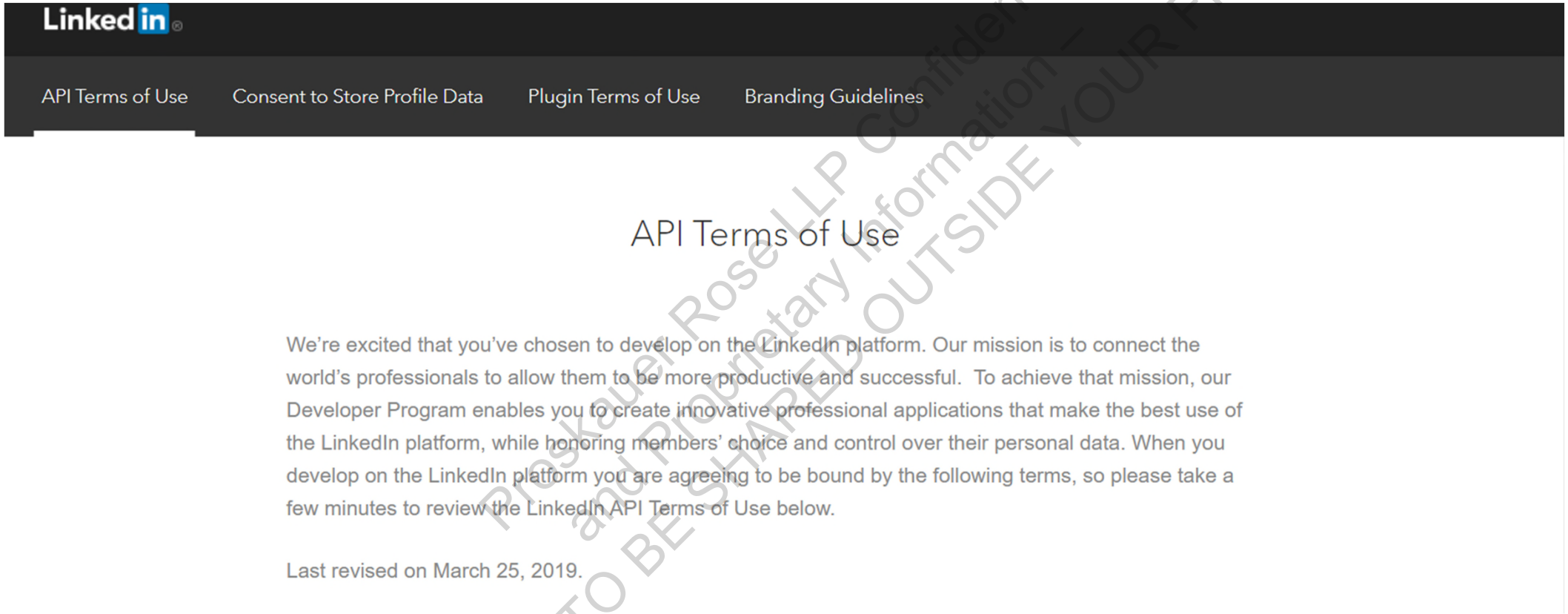
This would just be a script that I run for myself. I would only make money if the trades I make are successful (they probably won't be). However, if I make money, do I need your permission?

I'm not developing an app so there won't be any "in-app advertising" or "in-app purchases." You bet I "intend to learn from the data," but I'm not "repackag[ing] for sale." I don't have enough time to read every post/comment on this enormous group so I was hoping to automate some of the work for myself.

So, do I have your permission/approval to create this script/program? What exactly would the approval process be?

P.S. $GME to the Moon! 🚀🚀🚀🌙🌙

LinkedIn APIs



LinkedIn APIs

LinkedIn API Overview

LinkedIn's home for API documentation for all LinkedIn business lines. Our API documentation is organized by business lines covering Consumer, Compliance, Learning, Marketing, Sales, and Talent Solutions. Follow the links below to learn more about business lines and their possible integration types.

Where to Start

GET STARTED

- LinkedIn Business Solutions
- Get API Access
- Authentication
- API Concepts
- Breaking Change Policy
- Best Practices
- Error Handling

Consumer Solutions

OVERVIEW

- Consumer Overview
- Sign in with LinkedIn
- Share on LinkedIn
- Plugins

Learning Solutions

OVERVIEW

- Learning Home
- Learning Overview
- Request Access
- API Terminology
- API Foundations

Talent Solutions

OVERVIEW

- Talent Overview
- Recruiter System Connect
- Apply Connect
- Talent Hub
- Apply with LinkedIn
- Premium Job Posting
- Easy Apply

Sales Solutions

OVERVIEW

- Sales Overview
- Analytics Services
- Display Services
- Sync Services

Marketing Solutions

OVERVIEW

- Marketing Overview
- Getting Started
- Use Cases
- Integrations Overview
- Apply for Access
- Recent Changes

Compliance

OVERVIEW

- Compliance Overview
- Release Notes

LinkedIn APIs

adam4leos September 10, 2019 at 03:05 PM

Bypassing LinkedIn Search Limit by Playi

Original author: Adam Leos

JavaScript, API, Reverse engineering, Data storage, Social networks and communities

Translation

[Because my extension got a lot of attention from the foreign audience, I transl into English].

Limit

Being a top-rated professional network, LinkedIn, unfortunately, for free accounts, ha Commercial Use Limit (CUL). Most likely, you, same as me until recently, have never e heard about this thing.

Important Update — LinkedIn took into account this backdoor and fixed it. Backdoor and plugin do not working anymore.

1/ LinkedIn scraping best practices

Profile page extractions

❄️ **80 profiles** over **8 launches** of **10 profiles** each

🔥 **150 profiles** over **10 launches** of **15 profiles** each

💰 **300 profiles** over **20 launches** of **15 profiles** each

By profile, we mean any visit to a "Show" page. For instance, a company page, a profile page, a school page or a job page.

Search result extractions

❄️ Max **100 pages/1000 results** per day over **5 launches** minimum

🔥 Max **150 pages/1500 results** per day over **7 launches** minimum

💰 Sales Nav max **200 pages/5000 results** per day over **10 launches** minimum

LinkedIn searches display a **max** of 100 results pages. For searches resulting in thousands of results, you **cannot** scrape more than the first 1000 results with a regular LinkedIn account. Sales Navigator displays 25 results per page, so with these accounts you can scrape a **max** of 2500 results. To get every result, make

Call the Tax Lawyer….

4959

2021-2022 Regular Sessions

IN SENATE

February 19, 2021

Introduced by Sen. KRUEGER -- read twice and ordered printed, and when printed to be committed to the Committee on Investigations and Government Operations

AN ACT to amend the tax law, in relation to creating an excise tax on the collection of consumer data by commercial data collectors

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

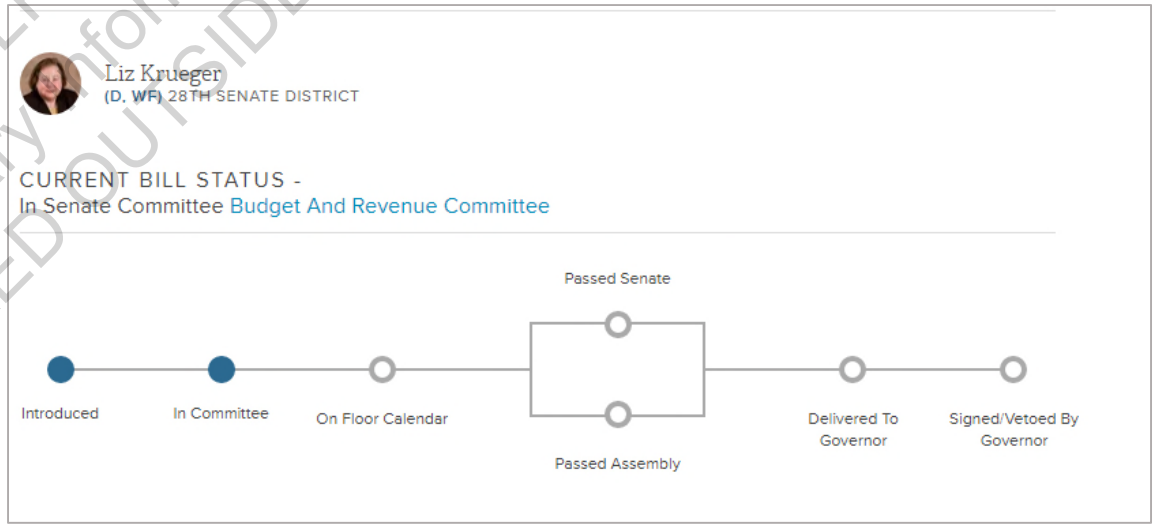
Section 1. The tax law is amended by adding a new section 186-h to read as follows:

§ 186-h. Excise tax on the collection of consumer data by commercial data collectors. 1. Imposition of tax. There is hereby imposed a monthly excise tax on the collection of the consumer data of individual New York consumers by commercial data collectors. The tax shall apply regardless of the format, electronic or otherwise, in which the consumer data is collected by the commercial data collector.

2. Definitions. As used in this section:

(a) The words "commercial data collector" mean a for-profit entity that:

(i) collects, maintains, uses, processes, sells or shares consumer data in support of its business activities; and



Proskauer's Big Data Breakfast

Robert Leonard
Michael Mavrides
Jeffrey Neuburger
Joshua Newville
Samuel Waldon
Christopher Wells

March 23, 2021

Thank You!!!

Proskauer