

# Hedge Funds Big Data Breakfast

Proskauer»

# Hedge Funds Big Data Breakfast

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

October 19, 2021

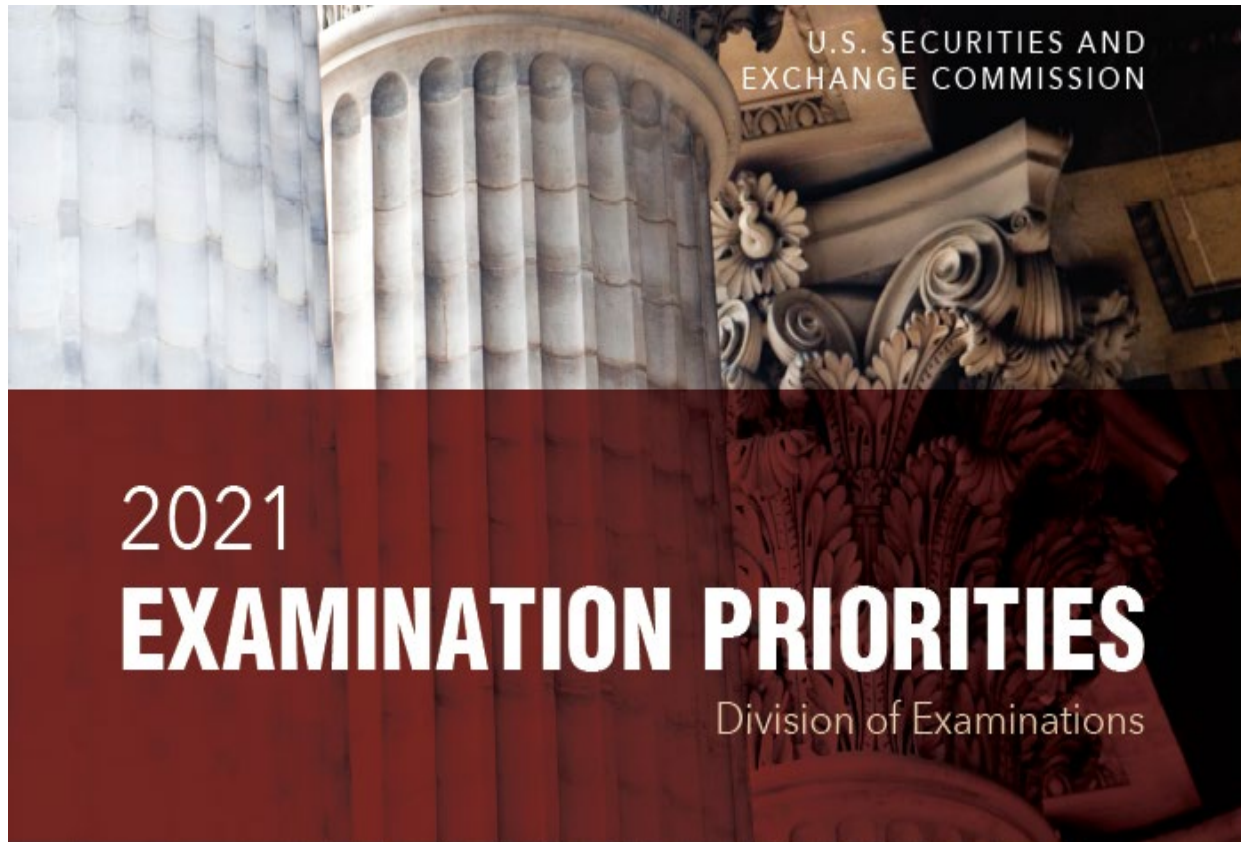
Proskauer»

# Today's Agenda

---

- **Recent SEC Views**
- **The App Annie Takeaways**
- **Locational Data**
- **Financial Data**
- **Mobile Data**
- **Scraping**
- **Antitrust and Other Political Issues**
- **Questions?**

# Regulatory Issues at the SEC



“**Alternative data**, or data gleaned from non-traditional sources, is increasingly being used by firms, including advisers to private funds and registered investment companies, as part of their business and investment decision-making processes. Reviews will include examining whether firms are implementing appropriate controls and compliance around the creation, receipt, and use of such information.”



# Alternative Data Exams

## Recent SEC Views

---

- Maintain written policies and procedures to vet alt data.
  - Include diligence for approvals/renewals
  - Approval/rejection criteria
  - Follow-up on red flags
  - Policies on web scraping
- Apply policies and procedures consistently
- Ensure DDQs are responded to, with all substantive questions answered in a meaningful way
- Do not rely on contractual reps to resolve open diligence questions.
- Require access to excerpts of relevant underlying consents, etc.

# The App Annie Takeaways....

## App Annie will pay \$10 million to settle a fraud investigation with the SEC

*Its former CEO will pay a \$300,000 fine, the agency said*

By Kim Lyons | @SocialKimLy | Sep 15, 2021, 9:45am EDT

f   SHARE



# App Annie – The SEC’s First Enforcement Action against an Alternative Data Provider

---

- App Annie and its ex-CEO represented to subscribers that the estimates of app performance contained in its Intelligence analytics product were generated using aggregated and anonymized app performance metrics. Instead, according to the SEC, App Annie used confidential, non-aggregated and non-anonymized app performance data to modify its estimates (which were generated by a statistical model) so as to make the Intelligence estimates closer to collected actual app metrics and more valuable to trading firms.
- The SEC’s order also found that App Annie/Schmitt misrepresented to Intelligence subscribers that App Annie had effective internal controls to prevent the misuse of confidential data and that no public company data would be used to generate the estimates.
- As part of the settlement, App Annie agreed to pay a \$10 million civil penalty and its former CEP agreed to pay a \$300,000 penalty and to be barred from serving as an officer or director of a public company for three years.
- Enforcement offers lessons on the risks for funds acquiring alternative data...

# App Annie Enforcement – Takeaways

---

- Enhanced diligence, policies and procedures
  - Walls between data provider confidential inputs and aggregated licensed data
  - Focus on who is responding in diligence reviews
  - DDQ certifications
  - Renewed diligence, contractual notice/termination triggers if...
    - Data quality changes +/-
    - Data sources change
    - Investigations



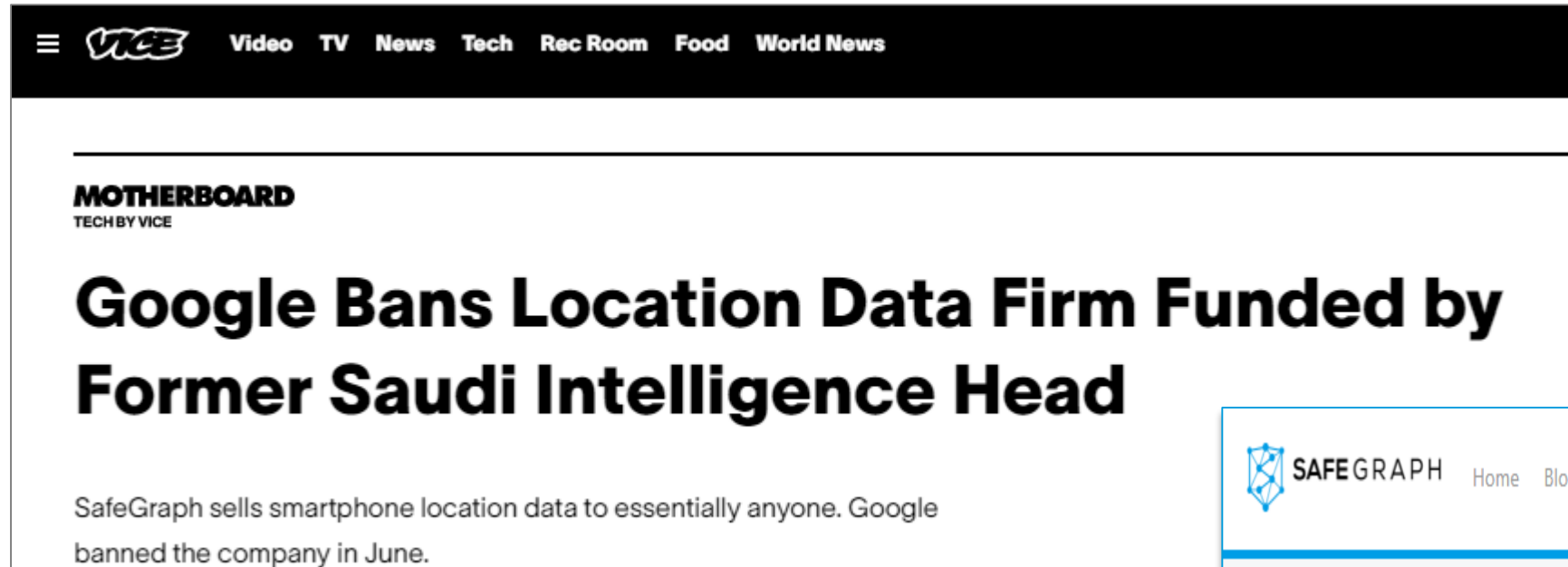
# App Annie – Additional Takeaways

---

- Action reflects an extremely broad view of “in connection with the purchase or sale of securities”
  - The SEC will certainly view any alleged misconduct by a fund manager to be “in connection with”
- This was not a tipping case, but if a fund manager knew or should have known about App Annie’s breach, it could have been.
  - Again, appropriate due diligence is critical
- What App Annie is saying today

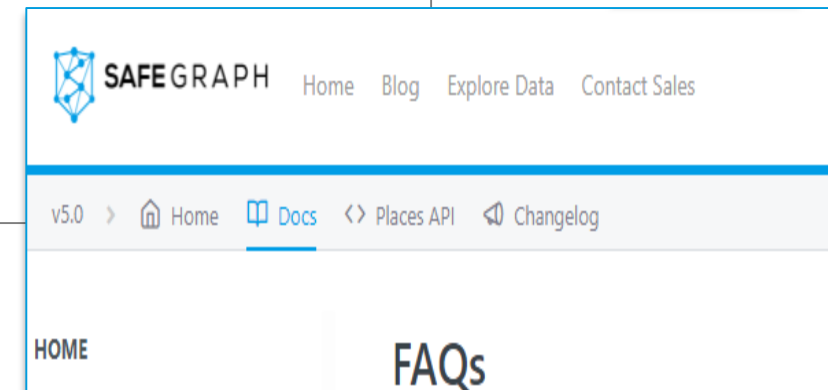
# Locational Data

## Google Tells Developers to Remove Apps with the SafeGraph SDK



But...

SafeGraph collected at least some of its location data by having app developers embed the company's code, or software development kit (SDK), into their own apps. Those apps would then track the physical location of their users, which SafeGraph would repackage and then sell to other parties. Google confirmed to Motherboard it told app developers in early June they had seven days to remove SafeGraph's SDK from their apps. If they didn't do this, Google told Motherboard the apps may face enforcement. This can mean removal from the Play Store itself.



Is there a SafeGraph SDK?

No. SafeGraph does not have an SDK or any software for that matter that can make it into mobile apps.

# Financial Data

## Consolidated Class Actions Against Plaid Tentatively Settled Aug. 6, 2021

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION

IN RE PLAID INC. PRIVACY  
LITIGATION

Master Docket No.: 4:20-cv-03056-DMR

**NOTICE OF MOTION AND MOTION  
FOR PRELIMINARY APPROVAL OF  
CLASS ACTION SETTLEMENT**

THIS DOCUMENT RELATES TO:  
ALL ACTIONS

**Sept. 30, 2021:** Hearing  
held and motion taken  
under submission

Date: Sept. 30, 2021  
Time: 1:00 p.m.  
Courtroom: via videoconference only  
Judge: The Hon. Donna M. Ryu

NOTICE OF MOTION FOR PRELIMINARY  
APPROVAL OF CLASS ACTION SETTLEMENT  
CASE NO. 4:20-CV-03056-DMR

# Financial Data

## Consolidated Class Actions Against Plaid Tentatively Settled Aug. 6, 2021

---

- \$58 million settlement fund
- Plaid will delete data that was retrieved as part of Plaid's "Transactions" feature
- Plaid agreed to change a number of its privacy and data collection practices (for at least three years within the U.S.), including:
  - (1) promises to inform how to use the Plaid Portal and manage the connections made between financial accounts and fintech apps;
  - (2) employ clear disclosures about Plaid's role when consumers link accounts to a fintech app;
  - (3) avoid using the particular bank's own color scheme in the credential pane
  - (4) require users to affirmatively agree to Plaid's privacy policy; and
  - (5) minimize the data Plaid stores (subject to certain limitations and exceptions)
- While a private class action, could this set a standard that the SEC looks to in similar data collection situations
- **Consider settlement points in due diligence process**

# Financial Data

## Similar Suit still pending...

---

*Wesch v. Yodlee, Inc.*, No. 20-05991 (N.D. Cal. July 29, 2021)

- **Claims:** Plaintiffs allege that Yodlee surreptitiously collect Plaintiffs' financial data from software products that it markets and sells to some of the large financial institutions, wealth management firms, and digital payment platforms like PayPal, which use Yodlee's software.
- **July 2021:** Several claims dismissed per Yodlee's motion to dismiss
- Claims pending include invasion of privacy and state misrepresentation claims
- Litigation remains ongoing
- **Oct. 2021:** Yodlee filed motion for Summary Judgment



# Financial Data

## Industry Migration to API-Based Solutions

---

AMERICAN BANKER

### The race to build data-sharing hubs for banks — and end screen scraping

By Penny Crosman September 20, 2021, 4:41 p.m. EDT 7 Min Read



The news last week that TD Bank's U.S. subsidiary will join the Akoya Data Access Network was a further sign of how the industry is trying to leave screen scraping in the dust.

Though banks have tried to hone the use of application programming interfaces for years, the most common way aggregators and fintechs access customer account data is still scraping the information with the use of a consumer's login credentials.

# General Mobile Data Issues – **Evolving Diligence Items**

## March 2022 – No App Inventory Features on Android



Effective March 1, 2022

Due to COVID-19 related considerations, enforcement for apps that target Android 11 (API level 30) and request `QUERY_ALL_PACKAGES` will not start until March 1, 2022.

Google Play restricts the use of [high-risk or sensitive permissions](#), including the `QUERY_ALL_PACKAGES` permission, which gives visibility into the inventory of installed apps on a given device. Play regards the inventory of installed apps queried from a user's device as personal and sensitive information, and the use of the permission is only permitted when your app's core use is for data visibility or business analytics based visibility into installed apps on the user's device.

If your app does not meet the requirements for acceptable use, you must update your app's manifest in order to comply with Play policy. Suggestions for acceptable use are also detailed below.

### Exceptions

### Invalid uses

Below is a list of use cases that won't be allowed to request the `QUERY_ALL_PACKAGES` permission:

- Where the use of the permission is not directly related to the core purpose of the app.
  - This includes Peer-to-Peer (P2P) sharing. P2P must be the core purpose of the app in order to qualify as a permitted use.
- When the data is acquired for the purpose of sale.
- When the required task can be done with a less broad app-visibility method.

**Note:** This list is not exhaustive. For in-depth guidance on alternative options and best practices, see [Package visibility filtering on Android](#).

# General Mobile Data Issues – **Evolving Diligence Items**

## Other Relevant Android/iOS Changes

[Play Console Help](#)   [Policy Center](#)

[Policy Center](#) > [Updates and Other Resources](#) > [Summaries](#)

- Effective October 28, 2021:
  - We're updating our [User Data policy](#) to prohibit linking persistent device identifiers to personal and sensitive user data or resettable device identifiers unless for pre-approved use cases.



### Account deletion within apps required starting January 31

October 6, 2021

The updates to App Store Review Guideline 5.1.1 last June provided users with greater control over their personal data, stating that all apps that allow for account creation must also allow users to initiate deletion of their account from within the app. This requirement applies to all app submissions starting January 31, 2022. We encourage you to review any laws that may require you to maintain certain types of data, and to make sure your app clearly explains what data your app collects, how it collects that data, all uses of that data, your data retention/deletion policies, and more as described in the guideline. Examples of this type of data include electronic health records, and sales and warranty records. Please also confirm that the app privacy information on your product page is accurate.

# Greater Data Collection Disclosures Coming to Android

## Preparing for Google Play's new safety section

28 July 2021

Posted by Suzanne Frey, VP, Product, Android Security and Privacy

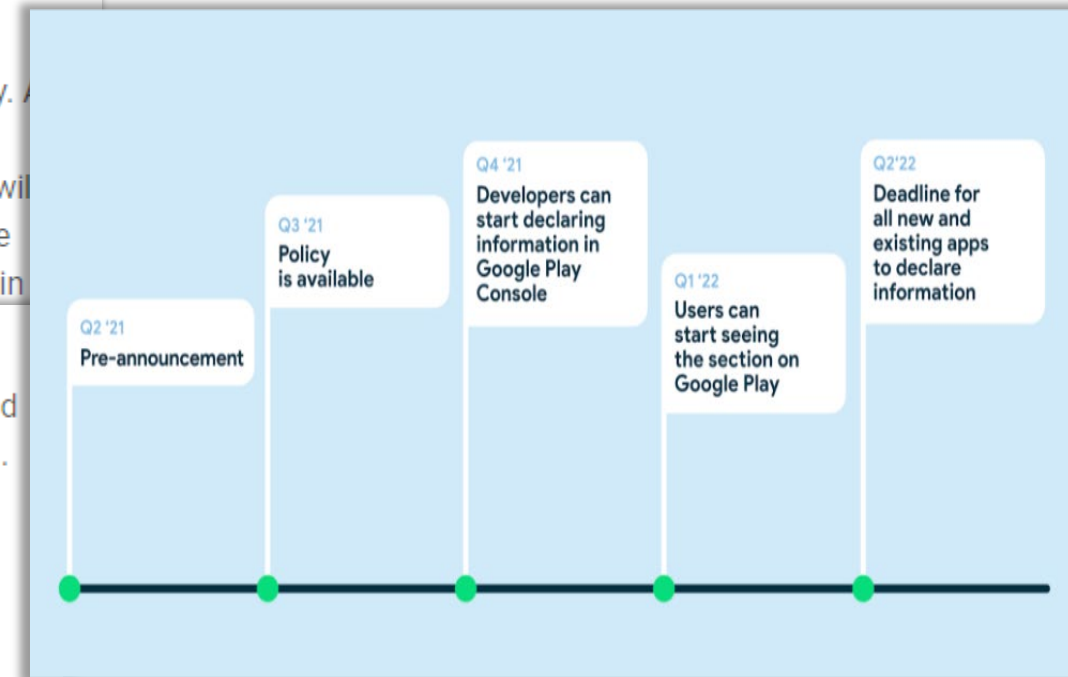
Today, we're announcing additional details for the [upcoming](#) safety section in Google Play. At Google, we know that feeling safe online comes from using products that are secure by default, private by design, and give users control over their data. This new safety section will provide developers a simple way to showcase their app's overall safety. Developers will be able to give users deeper insight into their privacy and security practices, as well as explain

### Policy changes to support the safety section

Today we announced new user data policies designed to provide more user transparency and to help people make informed choices about how their data is collected, protected and used.

- **All developers must provide a privacy policy.** Previously, only apps that collected personal and sensitive user data needed to share a [privacy policy](#).
- Developers are responsible for providing accurate and complete information in their safety section, including data used by the app's third party libraries or SDKs.

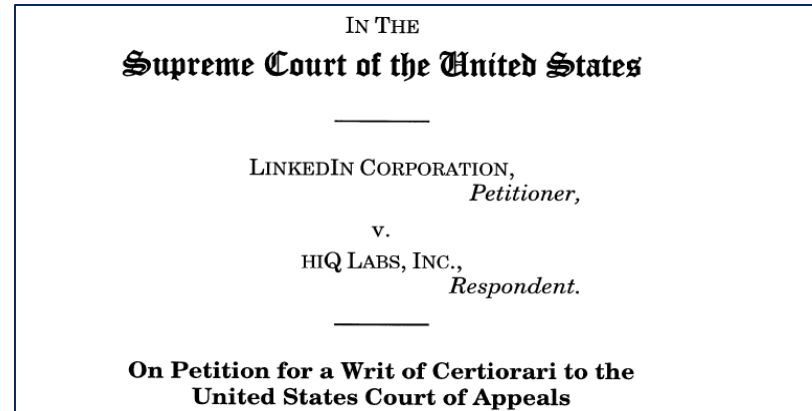
This applies to all apps published on Google Play, including Google's own apps.



# Scraping Developments

## The Latest on LinkedIn v. hiQ

***Cert. Granted, Ninth Circuit decision Vacated, Remanded for reconsideration***  
**Reconsideration based on Supreme Court decision in *Van Buren v United States***



**Ninth Circuit, 2019:** It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA.

**Issue to the Supreme Court:** Whether circumventing technical barriers and harvesting data from public-facing websites after the owner has expressly denied permission to access the data—“**intentionally accesses a computer without authorization**” in violation of the Computer Fraud and Abuse Act.



# Scraping Developments

## The Latest on LinkedIn v. hiQ

---

- Van Buren Supreme Court Decision: “Without authorization” is limited to those who access a computer without any authorization at all.
  - “**gates-up-or-down**” theory: “without authorization” ties to no authorization at access the system at all, while “exceeding authorized access” ties to accessing off-limits areas within the computer system.

***But what is a “gate”?***

**Van Buren, Footnote 8:** *“For present purposes, we need not address whether this inquiry turns only on technological (or code-based) limitations on access, or instead also looks to limits contained in contracts or policies.”*

# Oral Argument Heard by Ninth Circuit on Oct 18<sup>th</sup> Meanwhile...Public Profiles Subject of Scraping Attacks

JULY 19


Man behind LinkedIn scraping said he grabbed 700M profiles 'for fun'

Ben Lovejoy · Jul. 19th 2021 5:12 am PT [@benlovejoy](#)



CYBER SECURITY NEWS · 4 MIN READ

## "Combo File" Merging 3.8 Billion Phone Numbers from Clubhouse With Scraped Facebook Users Could Cause Surge in Phishing, Account Takeover Attacks

 SCOTT IKEDA · OCTOBER 1, 2021



Each taken on their own, the recent leaks of basic personal contact information from Clubhouse and Facebook users were not major security concerns. A new "combination file" offered on the dark web that makes connections between specific users of both platforms is more of a threat to create a spike in specific attack types, namely phishing and account takeover attempts.

## Data from 500M LinkedIn Users Posted for Sale Online

## Clubhouse data breach: 1.3 million users have info leaked online

By Balakumar K, Mike Moore April 12, 2021

But company denies claims it was hacked

# Oral Argument Heard by Ninth Circuit on Oct 18<sup>th</sup>

## Meanwhile... *Brooks v. Thomson Reuters*, (N.D. Cal. Aug. 16, 2021).

- Claims: Thomson Reuters CLEAR database assembles a vast array of individuals' PI scraped from public (and non-public) databases without consent of the data subject.
- Class action complaint – common law privacy and consumer protection claims
- Court declined to dismiss
  - “That some of Plaintiffs' personal information on the CLEAR dossiers comes from publicly available sources does not diminish the significant harm Plaintiffs suffer from the sale of that compiled information to whomever is willing to pay for it.”

### Privacy suit over Thomson Reuters database advances

*A judge emphasized that Thomson Reuters uses the database to sell subscriptions to private entities, rather than for journalistic purposes.*

MATTHEW RENDA / August 16, 2021



# Oral Argument Heard by Ninth Circuit on Oct 18<sup>th</sup> Meanwhile...Clearview AI Loses First Amendment Defense

## Lawsuit Challenges Clearview's Use of Scraped Social Media Images for Facial Recognition

Databases of involuntarily supplied identities make for a plug-and-play surveillance state.

### Judge: Clearview AI Cannot Use First Amendment as Defense in ACLU's Privacy Suit



by CHRISTINA TABACCO AUGUST 30, 2021

Late last week, an Illinois state court ruled in favor of the American Civil Liberties Union (ACLU) and other advocacy rights groups in their fight against Clearview AI Inc. over its unauthorized collection of Illinois residents' faceprints. According to the [order](#), the court has jurisdiction over the matter and the Illinois Biometric Information Privacy Act (BIPA) claims will proceed, despite Clearview's proffered free speech defense.

# Scraping Developments

## The Latest on LinkedIn v. hiQ

---

- **Sept. 2021:** LinkedIn files motion to dissolve the 2017 preliminary injunction enjoining LinkedIn from blocking hiQ's access to public profiles on LinkedIn's website because:
  - With recent mass scraping “attacks,” the equities have changed.
    - *“Events that have transpired in the nearly two years since this Court issued its opinion cast serious doubt on the Court’s evaluation of the equities and the public interest. The harms from mass-scraping of social media sites by entities like Clearview AI have shown that this Court’s skepticism that Internet users care about the privacy of their personal information was misplaced.”*
- Claims HiQ is no longer operational, and can no longer claim that it would suffer an irreparable injury in the absence of preliminary injunctive relief.
- Court deferred its ruling on the motion, in light of scheduled 9<sup>th</sup> Circuit argument.



# Scraping Developments

## LinkedIn v. hiQ: *Reargument Was on Oct 18<sup>th</sup>*

---

- **hiQ:** “‘Gates-up-or-down approach’ consistent with conclusion that the “prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort.”
- **LinkedIn:** “By making a website open to the public, a website operator puts its ‘gates up’ and presumptively authorizes access to the general public to access the site’s servers. In two mutually reinforcing ways, however, LinkedIn here revoked hiQ’s authorization to access LinkedIn’s servers. First, it sent a targeted cease-and desist letter to hiQ, informing hiQ that it lacked authorization. Second, LinkedIn set up additional, targeted technical measures to block hiQ’s access to its servers.”
- **hiQ:** “[W]hile LinkedIn may argue that its cease-and-desist letter and ‘counter-bot measures’ equate to a ‘gate’ that is ‘down,’ that cannot be the case. Such an argument would require distinguishing between any member of the public and bots, which the CFAA does not support. Because any interpretation of the CFAA must be universally applicable, and the data at issue here unquestionably is public, the gate can only be ‘up.’”

# Scraping Developments

## LinkedIn v. hiQ: *Reargument Was on Oct 18<sup>th</sup>*

---

- Judge Wallace: Ninth Circuit wrote a “clear, understandable opinion.” He said “[w]hen I look at the Supreme Court decision, it seems to me that our previous holding that the CFAA does not proscribe accessing publicly available information on websites that anyone with interest can share, it just seems to me to make irrelevant the Supreme Court decision.”
- Judge Berg: “When you are talking about the World Wide Web, how can this be considered comparable to illegal hacking? You’re putting in the hands of the private sector the ability to criminalize conduct, which is essentially accessing just a publicly available website where the default is that it should be available for all to see.
- Judge Berzon: hiQ doesn’t use any “technical hocus pocus” to scrape. She noted that LinkedIn’s efforts to restrict access by blocking the company’s IP addresses isn’t really a barrier because hiQ could use other IP addresses to access LinkedIn.

# Scraping Developments

## LinkedIn v. hiQ: Possible Diligence Implications of 9<sup>th</sup> Cir. Decision

- Following Judge Berzon's thoughts, the ruling will ultimately hinge on what technical measures were taken to block access and whether a formal revocation of access truly "lowered the access gate" or whether the "gate" for public website content is always up.
- Possible focus on technology-based restrictions such as IP Blocks, Captchas and Robots.txt
- No impact on contractual or other claims which are proceeding.
  - Recall: In April 2021, the district court declined to dismiss LinkedIn's breach of contract claim, finding that it made a plausible claim that in addition to prior breaches of the terms, hiQ, whose access was terminated, may still be subject to the terms in the future based on hiQ's alleged use of the site.

# Scraping Developments

## Meanwhile, Legal Landscape for Scraping Continues to Evolve

---

### Southwest Airlines Wins Injunction Barring Travel Site from Scraping



By [Jeffrey Neuburger](#) on October 4, 2021

Posted in [Contracts](#), [Internet](#), [Online Commerce](#), [Screen Scraping](#)

On September 30, 2021, a Texas district court granted Southwest Airline Co.'s ("Southwest") request for a preliminary injunction against online travel site Kiwi.com, Inc. ("Kiwi"), barring Kiwi from, among other things, scraping fare data from Southwest's website and committing other acts that violate Southwest's terms. (*Southwest Airlines Co. v. Kiwi.com, Inc.*, No. 21-00098 (N.D. Tex. Sept. 30, 2021)). Southwest is no stranger in seeking and, in most cases, obtaining injunctive relief against businesses that have harvested its fare data without authorization – ranging as far back as the 2000s (See e.g., *Southwest Airlines Co. v. BoardFirst, LLC*, No. 06-0891 (N.D. Tex. Sept. 12, 2007) (a case cited in the current court opinion)), and as recently as two years ago, when we wrote about a [2019 settlement Southwest entered into with an online entity](#) that scraped Southwest's site and had offered a fare notification service, all contrary to Southwest's terms.

***Southwest Airlines Co. v. Kiwi.com, Inc.*, No. 21-00098 (N.D. Tex. Sept. 30, 2021)**

# Scraping Developments

## Meanwhile, Legal Landscape for Scraping Continues to Evolve

---

- Texas district court granted Southwest Airline's request for a preliminary injunction barring Kiwi from scraping fare data from Southwest's website.
- Texas court found that Southwest had established a likelihood of success on the merits of its **breach of contract claim**
- Rejected Kiwi's argument that Southwest was not entitled to an injunction based on the *hiQ* ruling re publicly available data.
  - **Court:** “The Court is not persuaded the *hiQ* case means that Southwest cannot establish a likelihood of success on the merits for its breach of contract claim. [...] The opinion acknowledges a plaintiff could have a breach of contract claim even in the absence of a CFAA violation.”
- **Diligence Issue:** Remember to consider “terms of use” issue.



# Scraping Developments: “Public Data”

*Compulife Software, Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020)



- Database of processed/analyzed public facts can be a protectable trade secret
- If defendant took a large enough portion of the database through “improper means” it could be a trade secret violation.

“The simple fact that the quotes taken were publicly available does not *automatically* resolve the question in the defendants favor.”

“Nor does the fact that the defendants took the quotes from a publicly accessible site automatically mean the taking was authorized or proper. Although Compulife has plainly given the world implicit permission to access as many quotes as *humanly* possible, a robot can collect more quotes than any human practicably could. So, while manually accessing quotes from Compulife’s database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be... “ [emphasis original]

“Even if quotes aren’t trade secrets, taking enough of them must amount to misappropriation of the underlying secret at some point [under Florida law].”

“The trade-secret owner’s ‘failure to place a usage restriction on its website’ did not automatically render the hacking proper.”

# Scraping Developments: “Public Data”

*Compulife Software v. Newman*, 959 F.3d 1288 (11th Cir. 2020); July 13, 2021

---

- Following remand, a bench trial was held before a magistrate judge in Nov. 2020; Order issued July 13, 2021
  - “Defendants’ subsequent use of the Term4Sale website in a way that was never intended, stealing a significant portion of Compulife’s data... constitutes improper means.”
  - “The volume of Compulife’s data that Defendants acquired during the scraping attack [43.5 million results] constituted such a significant compilation of information that “[d]erives independent economic value . . . from . . . not being readily ascertainable” as to warrant trade secret protection.”
- **Possible diligence issue:** But note, this case, as most trade secret cases, involved competitors.

# Political Focus on Data Collection – Privacy & Data Collection Now a Focus of Antitrust

**Big Tech platforms gathering too much personal information**: Many of the large platforms' business models have depended on the accumulation of extraordinary amounts of sensitive personal information and related data.

In the Order, the President:

- Encourages the FTC to establish rules on surveillance and the accumulation of data.

“It is also the policy of my Administration to enforce the antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially **as they stem from serial mergers, the acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects.**”

Photographer: Alex Wong/Getty Images

## Biden's Executive Order Links Data Collection to Competition

July 9, 2021, 4:17 PM

- President urges FTC to write consumer data privacy rules
- Privacy policy push comes as Congress stalls, states act



**Andrea Vitt**  
Reporter

President Joe Biden's push for Federal Trade Commission rules protecting consumer data privacy highlights ties between tech companies' power and the personal information they collect.

Biden urged the FTC to write rules governing “the surveillance of users” in a [wide-reaching](#) executive order on competition, singling out unfair data collection practices that could damage competition and consumer privacy.

### Documents

Document  
[Fact sheet](#)

# Government Regulation of Data – Senate Calls for Renewed Effort to Pass Bipartisan Data Privacy Law

- Echoing Biden's EO, Democratic Senators urged the FTC Chair to use the agency's authority to write consumer data privacy rules, and at least one FTC Commissioner agreed with such a proposal.
- Republican Senators insisted this was Congress's domain and instead urged Congress to pass its own comprehensive legislation in this area instead (and also grant the FTC more enforcement authority in the area).

## Senate Democrats call on FTC to fix data privacy 'crisis'

*'Consumer privacy has become a consumer crisis'*

By Makena Kelly | @kellymakena | Sep 20, 2021, 3:02pm EDT

f t SHARE

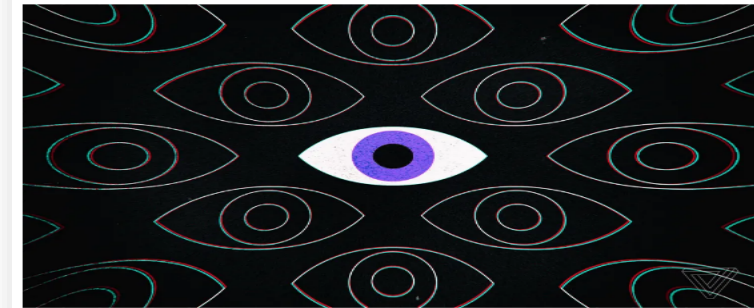


Illustration by Alex Castro / The Verge



Listen to this article

Senate Democrats are calling on the Federal Trade Commission to [write new rules](#) to protect consumer data privacy in a new letter to the agency authored on Monday.

## Sens. Turn Up Heat On Congress To Pass Federal Privacy Law

By Allison Grande

Law360 (September 29, 2021, 10:33 PM EDT) -- The top Republican on the U.S. Senate Commerce Committee on Wednesday railed against the [Federal Trade Commission's](#) push to use its powers to strengthen online privacy protections, asserting that only Congress has the authority to create such rules and backing a bipartisan call for lawmakers to enact a long-elusive federal privacy framework this year.

During a hearing held by the U.S. Senate Committee on Commerce, Science, and Transportation, Ranking Member Roger Wicker, R-Miss., agreed with his colleagues on both sides of the aisle that the FTC needs more resources and authority to crack down on companies that mishandle consumers' personal data. But he disputed a strategy being pursued under the commission's new Democratic majority to tap into a seldom-used rulemaking authority to [establish its own privacy and data security rules](#) to counteract Congress' inaction in this arena.

---

# CLE Verification Code

BL37YA

Questions About CLE? Contact:

Carolina Zardoya

212.969.5215

[czardoya@proskauer.com](mailto:czardoya@proskauer.com)



# Proskauer's Big Data Breakfast

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

October 19, 2021

Proskauer»

**Questions?**

**Thank You!!!**

# Hedge Funds Big Data Breakfast



The information provided in this slide presentation is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this presentation or any information contained on them. Rather, the content is intended as a general overview of the subject matter covered. Proskauer Rose LLP (Proskauer) is not obligated to provide updates on the information presented herein. Those viewing this presentation are encouraged to seek direct counsel on legal questions. © Proskauer Rose LLP. All Rights Reserved.