Proskauer's Big Data Breakfast

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

June 23, 2021

Proskauer

Agenda

- SEC Enforcement under Chairman Gensler
- The Alternative Data Tea Leaves under Gensler
- MNPI/Insider Trading
- An Update on LInkedIn v. HiQ and the implications of *Van Buren*
- Google/Android Policy Changes
- Apple Developments
- Federal Data Regulation – The Latest Proposal
- Facebook, Plaid and Google – Litigation Update
- GDPR – New Standard Contractual Clauses

SEC Enforcement Under Chairman Gensler

- Still early
  - Melissa Hodgman is still Acting Director of Enforcement
- Generally
  - More aggressive: more cases, higher penalties, more serious charges
  - Expect the SEC to be more willing to push aggressive theories and take on litigation risk
  - Much more control from the Chairman's office than in the past
  - More likely to see "rulemaking by enforcement"
  - Individual liability
  - Gatekeepers: lawyers, accountants, CCOs

SEC Enforcement Under Chairman Gensler

- Priorities so far
  - ESG, Crypto, market structure (meme stocks), SPACs
  - Wall Street rather than Main Street
- SolarWinds sweep -- first major initiative from Enforcement under Gensler

Reading the Gensler Tea Leaves on Alternative Data

- No clear guidance yet, but technology is clearly on the radar:
- Gensler on sentiment analysis:
  - "*Developments in machine learning, data analytics, and natural language processing have allowed sophisticated investors to monitor various forms of public communication to see relationships between words and prices. … With that comes the risk that nefarious actors may try to send signals to manipulate the market*."

    (May 6, 2021 House testimony)

Reading the Gensler Tea Leaves on Alternative Data

- Gensler on data analytics:
  - "*I believe we are only at the very beginning of our economy's growing reliance on the rapidly changing field of data analytics known as deep learning — a technology within artificial intelligence that is particularly adept at prediction and classification tasks. Our capital markets are no exception to this trend. We are starting to see AI-based funds, high-frequency traders, and asset management platforms, along with predictive tools and sentiment analysis*."
  - "*I believe these advancements also raise questions about the fairness, bias, and robustness of the individual analytic models themselves*."
  - "*I also think that as the financial sector matures in its use of deep learning in the capital markets, it's appropriate to consider how such data analytics may affect systemic risks*."

    (May 26, 2021 House testimony)

MNPI/Insider Trading

- SEC has brought fewer insider trading cases recently
  - Expect that to change
- *In the Matter of Andeavor* (Oct. 2020)
  - Two days before merger discussions, CEO directed a $250 million stock buyback, which was subject to company policy prohibiting repurchases while in possession of MNPI
  - Internal controls violations only: the company failed to maintain internal accounting controls providing reasonable assurance that the buyback complied with Andeavor's policy
  - No finding of violation of 10b-5/insider trading
  - $20 million penalty

MNPI/Insider Trading

- May 2021 - House (Re-)Passes the Insider Trading Prohibition Act:
  - Similar to version that passed the House in 2019.
- Bill would prohibit trading on MNPI that a person recklessly disregards was “obtained wrongfully”
- Wrongful defined as “if the information has been obtained by:”
  - (A) theft, bribery, misrepresentation, or espionage (through electronic or other means);
  - (B) a violation of any Federal law protecting computer data or the intellectual property or privacy of computer users;
  - (C) conversion, misappropriation, or other unauthorized and deceptive taking of such information; or
  - (D) a breach of any fiduciary duty, a breach of a confidentiality agreement, a breach of contract, a breach of any code of conduct or ethics policy, or a breach of any other personal or other relationship of trust and confidence for a direct or indirect personal benefit (including pecuniary gain, reputational benefit, or a gift of confidential information to a trading relative or friend).”

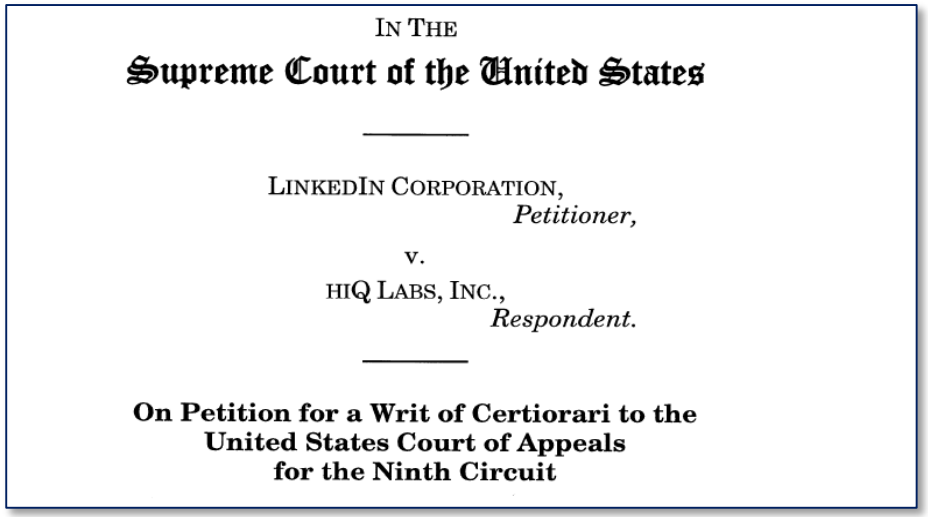
An Update on *LinkedIn v. hiQ* and its Implications for Web Scraped Alternative Data

Proskauer

An Update on *LinkedIn v. hiQ* and its Implications for Web Scraped Alt Data

Cert. Granted, Ninth Circuit decision Vacated, Remanded for reconsideration

Reconsideration based on Supreme Court decision in *Van Buren v United States*



IN THE

Supreme Court of the United States

LINKEDIN CORPORATION,
Petitioner,

v.

HIQ LABS, INC.,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

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 a company that deploys anonymous computer "bots" to circumvent technical barriers and harvest millions of individuals' personal data from computer servers that host public-facing websites—even after the computer servers' owner has expressly denied permission to access the data—"**intentionally accesses a computer without authorization**" in violation of the Computer Fraud and Abuse Act.

Background on *Van Buren v. United States*

- Police officer ran a database check through his department's system for personal favor in exchange for money. This was a violation of policy.
- Both parties agree that he accessed the computer with authorization.
- Computer Fraud and Abuse Act (CFAA) addresses situation where one "intentionally accesses a computer *without authorization* or *exceeds authorized access*."
- No question that he had authorization. Did he exceed authorized access?

Background on *Van Buren v. United States*

Definition of exceeds authorized access: “to access a computer with authorization and to use such access to obtain or alter information that the accesser is not entitled so to obtain or alter.”

What do you think? Did he “exceed authorized access” to his department’s computer system?

The Meaning of *"so"*

- **Definition of exceeds authorized access**: "to access a computer with authorization and to use such access to obtain or alter information that the accesser is not entitled ***SO*** to obtain or alter."
- Court: The use of the word "so" means "in the same manner that has been stated." Thus, the phrase could be construed as "…that the accesser is not **entitled to obtain by using a computer that he is authorized to access."**
- Court: It is undisputed that he was authorized to access the system. Exceeding authorized access only occurs on access to particular areas of the computer to which their authorized computer access does not extend (e.g., files, folders and databases).

Relevance to *LinkedIn* and Scraping

LinkedIn was brought under the "without authorization" prong of the CFAA.

Court: "Without authorization" is limited to those who access a computer without any authorization at all.

- Court adopts the defendant's "**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"?

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."***

A Few Other Interesting Points

"Under the dissent's approach, an employee's computer access would be *without* authorization if he logged on to the computer with the purpose of obtaining a file for personal reasons."

"Many websites, services, and databases … authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers."

Relevance to *LinkedIn* and Scraping

- On remand to the Ninth Circuit, the ruling will likely hinge on whether technical measures to block hiQ's access to LinkedIn's site and a formal revocation of access truly lowered the access gate or whether the "gate" for public website content is always up.
- In its Supplemental Brief filed with the Court following the *Van Buren* decision, LinkedIn argued that it had placed "gates" around its servers by using code-based technical measures to block bots and scraping activities, and its contracts and policies, as well as by sending a cease-and-desist letter revoking access.
- **Possible Implications for scraping and the CFAA**:
  - Possible clarity on "gates" of various types to come from the Ninth Circuit
  - Likely that websites will seek ways to present technological "gates" -- access restrictions -- on at least particular files/pages/databases on their sites
  - Refocus on code-based restrictions such as IP Blocks, Captchas and Robots.txt
  - **Diligence: Specific questions regarding circumventing access restrictions**

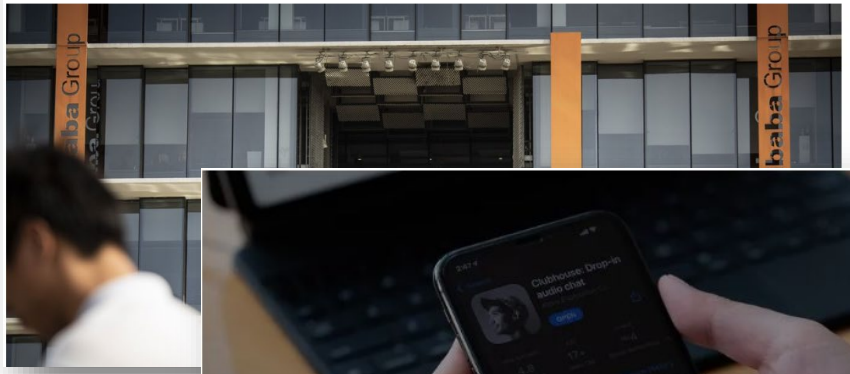
Meanwhile, in the District Court, the *hiQ* Case Continues…

- **Sept. 2020:** Judge dismissed hiQ's antitrust claims against LinkedIn
- **Nov. 2020**: LinkedIn files Answer with Counterclaims (incl. CFAA, breach of contract and misappropriation)
- **Apr. 2021**: Court denies hiQ's motion to dismiss LinkedIn's Counterclaims:
  - **CFAA**: Court deferred ruling until *Van Buren* decision was released.
  - **CDAFA**: Calif. computer trespass law (similar to CFAA) – court deferred until the *Van Buren* ruling.
  - **Contract**: hiQ argued that LinkedIn terminated its user status, thus no breach claim; LinkedIn countered that the terms govern active users and those who simply use the site, and since hiQ used the site following its termination with actual knowledge of the terms that are linked at the bottom of each page, it is bound by the terms. Court ruled that: "LinkedIn has a basis for arguing that, if hiQ has actual notice of the terms of the User Agreement (which contains, e.g., a prohibition against scraping), it can be subject to those terms."
  - **Misappropriation**: Allowed to continue; questions of fact remain as to whether hiQ is a "free rider"
  - **Trespass to Chattels**: Court found LinkedIn asserted a plausible claim, based on interference with servers and the possibility that others will mimic such scraping and cause future harm to LinkedIn.

In the Meantime…

Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak

Software developer scrapes 1.1 billion pieces of user data, including IDs and phone numbers, over eight months



DATA PRIVACY NEWS · 4 MIN READ

Clubhouse Joins Facebook and LinkedIn as Target of Data Scraping; Cumulative One Billion User Profiles Have Been Leaked

SCOTT IKEDA · APRIL 16, 2021

Trove of Online LinkedIn User Data Fuels LinkedIn's Anti-Scraping Position

By **Jeffrey Neuburger** on April 13, 2021
Posted in **Computer Fraud and Abuse Act, Data Security, Privacy, Screen Scraping, Social Media**

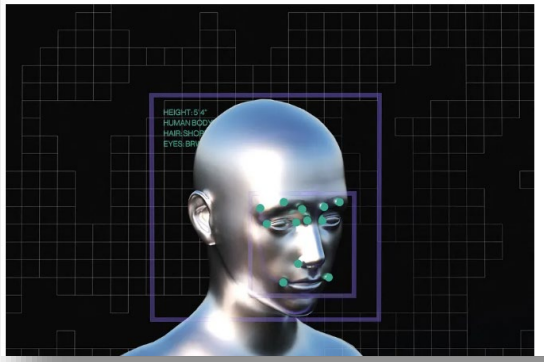
Last week, the Italian data protection authority (the "GPDP") opened an investigation after reports that a dataset allegedly containing data compiled from 500 million LinkedIn profiles and other websites was available for sale on a hacker forum. Apparently, this data represents more than two-thirds of LinkedIn's estimated 740 million users. The hacker reportedly posted approximately two million records visibly online as evidence of the dataset, and offered to sell the rest for an undisclosed bitcoin payment.

Is there any way out of Clearview's facial recognition database?

The maddening logic of facial recognition

By Dave Gershgorn | Jun 9, 2021, 10:30am EDT

SHARE



Hacktivist Posts Massive Scrape of Crime App Citizen to Dark Web

The cache includes data on 1.7 million incidents, giving insight into the scale of Citizen around the country.

By Joseph Cox

May 26, 2021, 11:22am Share Tweet Snap

Proskauer

Google/Android Policy Changes

developers Platform Android Studio Google Play Jetpack More Search English

Overview Play Console Play Store Play Billing Play Policies Play Services Games Guides Stories

Policy page Declaration form tips

Comply with March policy updates

We're updating Google Play Policies, including our policy related to All Files Access permission, and adding new examples and clarifications to some of our policies. New and existing apps have until May 5th, 2021 to comply.

Google “Clarifications” to Policies – March 31, 2021

Personal and Sensitive Information

Personal and sensitive user data includes, *but isn't limited to*, personally identifiable information, financial and payment information, authentication information, phonebook, contacts, *device location*, SMS and call related data, *inventory of other apps on the device*, microphone, camera, and *other sensitive device or usage data*. If your app handles sensitive user data, then you must: …..

- Limit your access, collection, use, and sharing of personal or sensitive data acquired through the app to purposes directly related to providing and improving the features of the app (e.g., user anticipated functionality that is documented and promoted in the app's description in the Play Store). Apps that extend usage of this data for serving advertising must be in compliance with our Ads Policy.

Google “Clarifications” to Policies – March 31, 2021

If your app handles sensitive user data, then you must:

- Post a privacy policy in both the designated field in the Play Console and within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app accesses, collects, uses, and shares user data. Your privacy policy must disclose the types of personal and sensitive data your app accesses, collects, uses, and shares; and any parties with which any personal or sensitive user data is shared.

Google “Clarifications” to Policies – March 31, 2021

Examples of common violations:

- An app that accesses a user's inventory of installed apps and doesn't treat this data as personal or sensitive data subject to the above Privacy Policy, data handling, and Prominent Disclosure and Consent requirements.
- An app that collects device location and does not comprehensively disclose its use and obtain consent in accordance with the above requirements.

Greater Data Collection Disclosures Coming to Android

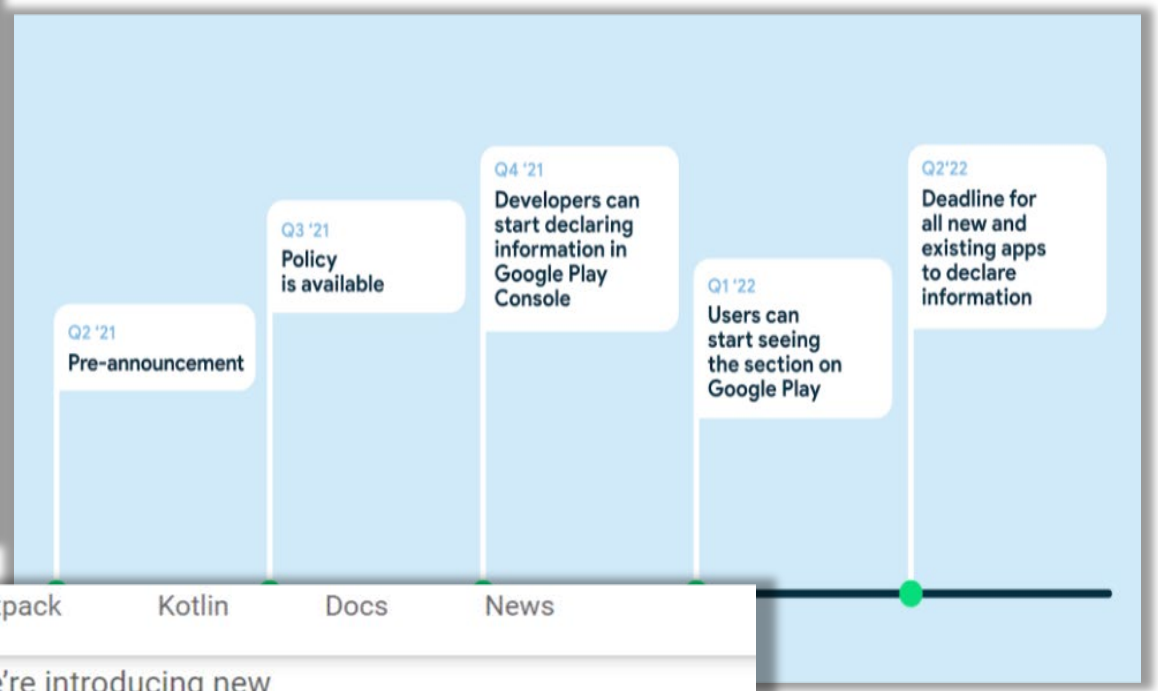
Android Developers Blog

The latest Android and Google Play news for app and game developers.

New safety section in Google Play will give transparency into how apps use data

06 May 2021

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



developers Platform Android Studio Google Play Jetpack Kotlin Docs News

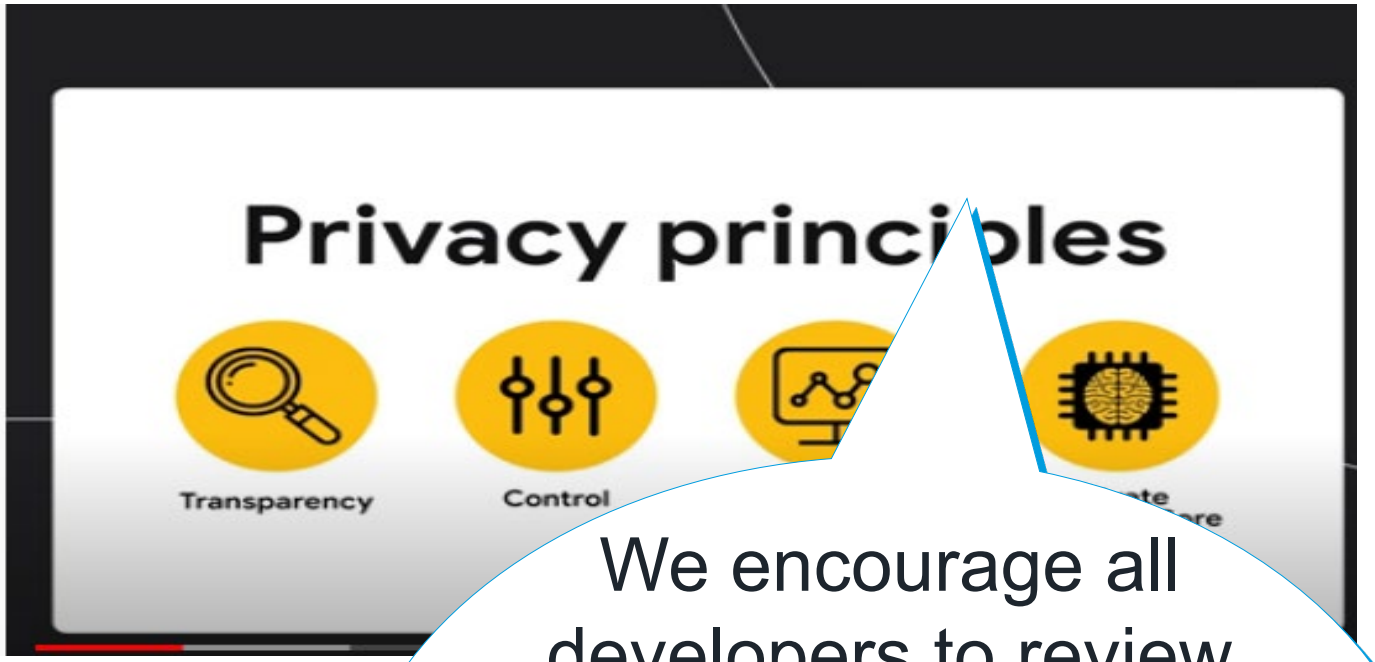
experience. So in addition to the data an app collects or shares, we're introducing new elements to highlight whether:

1. The app has security practices, like data **encryption**
2. The app follows our **Families policy**
3. The app needs this data to function or **if users have choice** in sharing it
4. The app's safety section is **verified** by an independent third-party
5. The app enables users to request data deletion, if they decide to uninstall

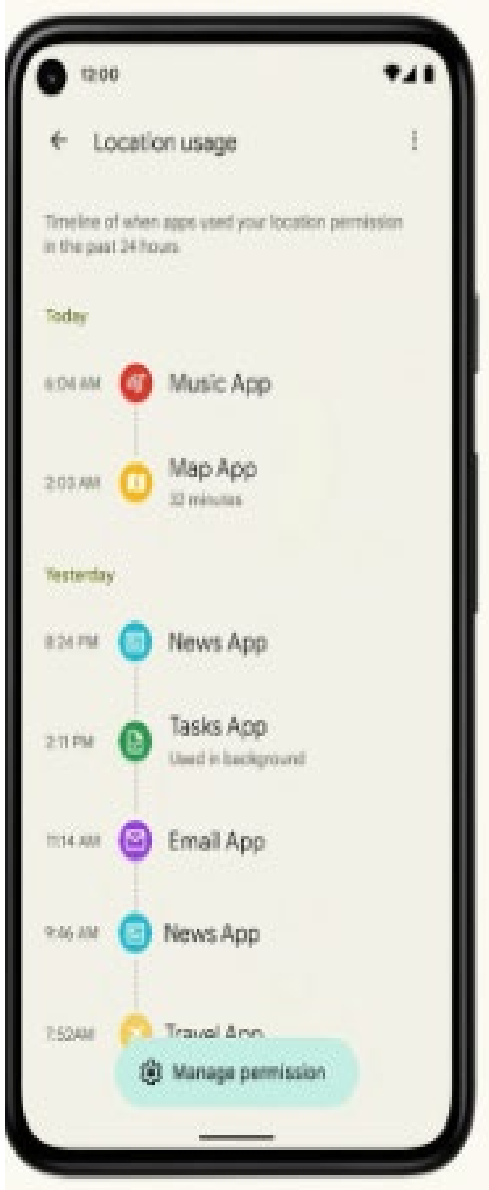
This can be a big change, so we're sharing this in advance and building with developers alongside us.

Proskauer

Android 12, August 2021



We encourage all developers to review your code…including ..third party SDKS and make sure all accesses have justifiable use cases.



Proskauer

What's happening with Apple and iOS?

App Store Review Guideline updates now available

June 7, 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.

Read more ›

Apple App Rejections in 2020

- Rejected about 1 million apps, and about 1 million app updates.
- 48,000 apps were removed for using “hidden or undocumented features.”
- 150,000 apps were removed because they were spam or copied another app.
- 215,000 apps were removed because they collected too much user data or other privacy violations.
- 95,000 apps were removed for fraud, often because they changed after Apple’s review to become a different kind of app, including gambling apps or pornography.
- Apple booted 470,000 accounts from its developer program because of fraud.
- In addition, Apple said that last month, it rejected 3.2 million installations of apps that use an enterprise certificate, which is a way to evade the App Store.

Apple iOS 15

- Apple will by default block users' internet protocol addresses from being transmitted to trackers on websites visited in its Safari browser. Many companies collect a user's IP address and combine it with other data to "fingerprint" and recognize a user's repeat visits.

BUSINESS | MEDIA & MARKETING

Apple's Moves to Tighten Flow of User Data Leave Advertisers Anxious

Brands and ad-tech firms say tech giant's push to limit how users are tracked will hurt business, with some questioning privacy rationale

Data Legislation

KIRSTEN GILLIBRAND
UNITED STATES SENATOR FOR NEW YORK

ABOUT NEWS HELP CONTACT

NEWS / PRESS

June 17, 2021

Gillibrand Introduces New And Improved Consumer Watchdog Agency To Give Americans Control Over Their Data

Strengthened Data Protection Agency (DPA) Proposal Establishes Office of Civil Rights; Has Authority to Oversee Big Tech Mergers; US Is One of the Only Democracies Without A Dedicated Digital Protection Agency; Would Better Prepare the U.S. for the Digital Age

U.S. Senator Kirsten Gillibrand today announced her renewed legislation, the *Data Protection Act of 2021*, which would create the Data Protection Agency (DPA), an independent federal agency that would protect Americans' data, safeguard their privacy, and ensure data practices are fair and transparent. First introduced in 2020, the updated legislation has undergone significant improvements, including

Facebook and Scraping

HOME > TECH

533 million Facebook users' phone numbers and personal data have been leaked online


FACEBOOK Who We Are What We Build Ou

Facebook

The Facts on News Reports About Facebook Data

April 6, 2021

By Mike Clark, Product Management Director

Scraping is a common tactic that often relies on automated software to lift public information from the internet that can end up being distributed in online forums like this. The methods used to obtain this data set were previously reported in 2019. This is another example of th ongoing, adversarial relationship technology companies have with fraudsters who intentionally break platform policies to scrape internet services. As a result of the action we took, we are confident that the specific issue that allowed them to scrape this data in 2019 no longer exists. But since there's still confusion about this data and what we've done, we wanted to provide more details here.

Facebook and Scraping….

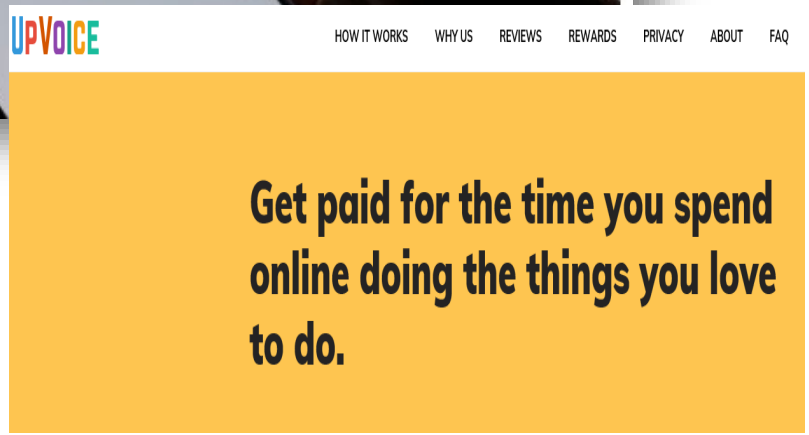
- We built an External Data Misuse team that consists of more than 100 people dedicated to detecting, investigating and blocking patterns of behavior associated with scraping.
- We impose rate and data limits, which are designed to restrict how much data a single person can obtain through a certain feature, and put other obstacles in place against unauthorized automation. We block billions of suspected scraping actions per day across Facebook and Instagram.
- We work with researchers to find and secure publicly accessible datasets that contain Facebook user data — whether the data appears to have originated from Facebook or a Facebook app developer. These datasets are found across a range of hosting providers and online platforms. The malicious actors who trade or sell these datasets often recycle or manipulate them over time, which means that many of them often contain duplicate information or inaccurate data.
- If we find scraped datasets containing Facebook data, there are no surefire options for getting them taken down or going after those responsible for them, but we may take a number of actions.
- In the past year, we've taken over 300 enforcement actions against people who abuse our platform, including sending cease and desist letters, disabling accounts, filing lawsuits or requesting assistance from hosting providers to get them taken down. In a recent case, we successfully reached a settlement with the operator of a service that violated our Terms

Proskauer

The Facebook – BrandTotal Case

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 includng 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.



Meanwhile: BrandTotal made changes to its browser extension during the litigation: **UpVoice 2021 does not collect users' demographic data from Facebook, instead relying on users to enter that information in a form when they sign up for the program**.

Facebook & Harvesting of Call and Text Logs

Williams v. Facebook Inc., No. 18-01881 (N.D. Cal. May 14, 2021)

- Plaintiffs claim that Facebook, via mobile apps, surreptitiously collected users' call and text logs, in violation of the California Invasion of Privacy Act ("CIPA"), which generally prohibits eavesdropping on *contents* of communications.
- Court dismissed the complaint again, finding that CIPA protects the "contents" of communications, not the call and text metadata.

Facebook Dodges Android Users' Data Scraping Suit, Again

By Hannah Albarazi

Law360 (May 17, 2021, 6:12 PM EDT) -- A California federal judge tossed a proposed class action accusing Facebook of surreptitiously scraping Android users' call and text logs and then selling that data to advertisers, ruling Friday that the Facebook users' third amended complaint still doesn't prove Facebook's scraping of metadata was unlawful.

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

DEMAND FOR JURY TRIAL

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Proskauer

A proposed class action alleged Plaid scraped financial and personal information from apps that used the company's software.

Photographer: Chris Ratcliffe/Bloomberg

Plaid Sheds Some Scraping Claims But Still Faces Privacy Suit

PLAID

TD Bank, Plaid Settle Trademark Suit, Seek Court Dismissal

Plaid forms open finance partnership with Capital One

10 June 2021 0 0 0

Source: Plaid

Last year, Plaid announced a goal to commit 75% of our traffic to APIs by the end of 2021.

This target for fair, reliable, and secure API-based data exchange is one of our top priorities as the industry moves full-steam ahead towards a fully digital financial system.

Because of the sustained efforts towards open finance, we have completed or have in-motion data access agreements with the majority of major U.S. financial institutions, including U.S. Bank, JPMorgan Chase, Wells Fargo, and others. Moving to an API-based ecosystem helps make data sharing more reliable, and also helps eliminate the industry's reliance on credentials, a major priority for us and the broader ecosystem.

As part of the arrangement, Plaid is in the process of deleting all Capital One customer credentials from its systems.

Proskauer

Update: Google Still Facing Handful of Locational Data 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.

Android Users Accuse Google Of Spying To Build Next TikTok

By *Dave Simpson*

Law360 (August 6, 2020, 7:53 PM EDT) -- Google LLC is monitoring Android smartphone users without their knowledge and harvesting their data, which the search giant intends to use to create a competitor to the short-form video app TikTok, according to a putative privacy class action filed in California federal court Wednesday.

Google Again Seeks Toss Of Users' Secret Tracking Suit

By *Lauren Berg*

Law360 (September 1, 2020, 6:59 PM EDT) -- Google urged a California federal judge Monday to toss for good a proposed class action accusing the tech giant of unlawfully tracking and storing users' private location information, arguing the users' latest complaint doesn't improve their "vague, boilerplate" allegations.

U.S. District Judge Edward J. Davila in June refused to rethink his decision to ax the suit, but the judge allowed the users to try again on allegations that Google's data collection violated California's constitution and users' common law right to privacy.

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 judge in California has stated that Google can be sued for collecting data on users even when they use "private browsing mode" on their selected browsers.

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

Proskauer

Final Note on EU Privacy Developments

- The European Commission adopted two sets of standard contractual clauses (SCCs), one for use between controllers and processors and one for the transfer of personal data to third countries.
  - SCCs are template data transfer agreements that allow data exporters to transfer data to countries outside the EEA that the European Commission identifies as providing an “inadequate” level of data protection (e.g., U.S., Australia, Brazil, China, India).
  - They take into account the GDPR and *Schrems II* judgment and offer more legal predictability to European businesses and help, in particular, SMEs to ensure compliance with requirements for safe data transfers, while allowing data to move freely across borders, without legal barriers.
  - More flexibility for complex processing chains, through a ‘modular approach' and by offering the possibility for more than two parties to join and use the clauses
  - The updated SCCs have *Schrems II* (C-311/18) in mind, requiring companies that use SCCs to undertake a “transfer impact assessment” to determine if so-called “supplementary measures” (e.g., encryption) need to be put into place (in addition to those measures required by the SCCs) in light of the laws of the country of data import.

CLE Verification Code

J8L92H

Questions About CLE? Contact:

Kristen Sidebottom
973.681.6341
ksidebottom@proskauer.com

Proskauer

Proskauer's Big Data Breakfast

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

June 23, 2021

Thank You!!!

Proskauer