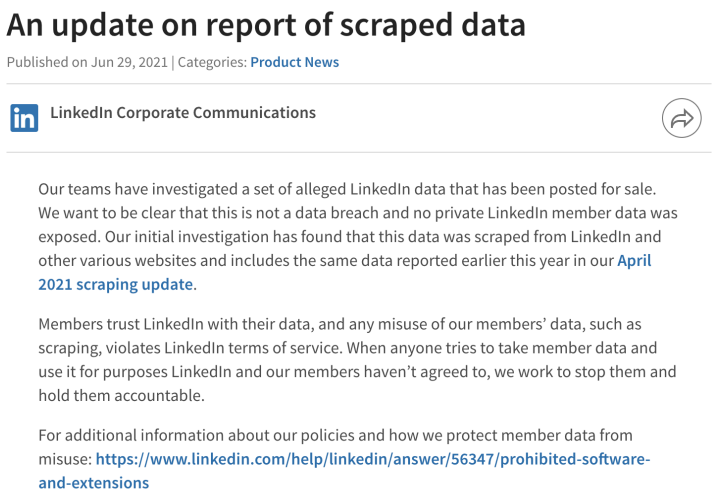
2021 LinkedIn API Exploitation

The paper discusses the 2021 LinkedIn data breach involving the scraping of personal information through LinkedIn's API, which were compiled into a super-list and sold on the dark web.
This incident aggregated personal data from nearly 92% of its users. A massive amount of personal information was exposed including names, email addresses, phone numbers, physical addresses, and professional details, enabling further social engineering attacks. Users with a background in technology, software development, or digital privacy may be more aware that APIs can access user data for various legitimate purposes, such as app integration and functionality enhancement. However, they might not fully anticipate the scale at which data can be scraped or aggregated for unauthorized uses. Moreover, like many social media platforms, outlines in its user agreement and privacy policy how user data can be accessed and used, including through its API. Yet, these documents are often lengthy, complex, and not thoroughly read or understood by the average user, potentially leading to gaps in user awareness about their data's accessibility and vulnerability.

Reference: https://ieeexplore.ieee.org/document/9799221

LinkedIn's Response



An update on report of scraped data

Published on Jun 29, 2021 | Categories: Product News

LinkedIn Corporate Communications

Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed. Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our April 2021 scraping update.

Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.

For additional information about our policies and how we protect member data from misuse: https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions

Reference: https://news.linkedin.com/2021/june/an-update-from-linkedin

2023 Massive LinkedIn Data Scraping Incident

Shortly after a significant Facebook data breach, LinkedIn experienced a similar security incident, with data from 500 million profiles allegedly scraped and put up for sale on a hacker forum. An additional 2 million records were leaked as a sample. The exposed information includes LinkedIn IDs, full names, email addresses, phone numbers, professional titles, and other work-related data. LinkedIn clarified that this incident did not result from a data breach of their systems but was an aggregation of data from various sources, suggesting the data might be outdated or duplicated. Following this incident, Italy's privacy watchdog initiated an investigation, given the country's large number of LinkedIn users. Another threat actor later claimed to have a larger dataset of 827 million profiles, exceeding LinkedIn's total user

base, indicating possible duplicates or outdated information. Users are advised to check if their data was compromised, change passwords, enable two-factor authentication, and be cautious of phishing attempts.

Reference:
https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2-million-leaked-as-proof-2/

FTC's Historic $5 Billion Settlement with Facebook

The FTC imposed a record $5 billion penalty on Facebook for violating a 2012 order by misleading users about their privacy controls, marking the largest privacy-related fine ever. This settlement mandates sweeping changes to Facebook's privacy practices and corporate structure to enhance accountability and transparency. New requirements include the establishment of an independent privacy committee, designated compliance officers, and stringent compliance certifications by CEO Mark Zuckerberg. The order also introduces strict oversight mechanisms for third-party apps, enhanced user consent for facial recognition, and comprehensive data security protocols. This action represents a significant effort by the FTC to enforce privacy protections and ensure Facebook's adherence to user privacy commitments.

Reference:
https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Walmart Sued for Non-consensual Data Sharing

Two Walmart customers filed a class-action lawsuit against the retail giant, alleging unauthorized disclosure of their personal data, including Facebook accounts and purchase information, when buying video content on Walmart.com. The suit claims Walmart violated U.S. and California privacy laws by using a Facebook pixel on its website, a tool that leverages cookies for advertising and analytics. While Walmart stated it takes customer privacy seriously and is reviewing the allegations, the case highlights ongoing concerns around consumer data privacy in e-commerce, emphasizing the need for retailers to consider consumer privacy concerns and protective measures seriously.

Reference: https://www.retaildive.com/news/walmart-sued-over-use-of-customer-data-online/539429/

Health Apps Share User Data with Insurance Firms

A study highlighted privacy concerns with the health apps market, revealing that 20 popular health-tracking apps are sharing user data with nearly 70 advertising and analytics companies. The data shared includes personal information gathered from users' activities on apps like MapMyRun, Lose It!, and Period Tracker. This sharing of data is raising alarms not just for its privacy implications but also for the interest it sparks in insurance companies. Large insurance firms are entering partnerships with health app developers, with services like Aetna's CarePass explicitly linking health apps to insurance offerings, allowing users to control which apps connect to their health data. However, the transparency around such partnerships and data sharing practices remains a concern, especially as the health apps industry grows

and becomes a significant interest area for insurance companies looking to harness big data for personalized insurance policies. This situation underscores the need for greater clarity on how health-related data is used and shared, particularly with entities like insurance companies that could use the data to impact insurance terms or premiums.

Reference:
https://www.theguardian.com/technology/appsblog/2013/sep/03/fitness-health-apps-sharing-data-insurance

Risky Driving? Insurance Apps Could Increase Your Premiums

In recent years, drivers in Canada have had the opportunity to lower their auto insurance premiums through apps or telematics devices that track safe driving habits or limited vehicle usage. However, changes in regulations across several provinces, including Ontario, Quebec, and Alberta, now allow insurers to also increase premiums based on risky driving behaviors or high mileage detected by these tracking technologies. These adjustments aim to provide more choice and flexibility for consumers, rewarding safe drivers with lower rates while penalizing high-risk behaviors with higher premiums. Despite the potential savings and increased adoption during the COVID-19 pandemic, privacy concerns persist about the continuous data gathering by these usage-based insurance programs. Consumers are advised to fully understand the terms and consider potential surcharges before opting into such programs. Insurers argue that usage-based insurance could lead to safer roads by incentivizing better driving behavior.

Reference:
https://globalnews.ca/news/7704732/auto-insurance-app-usage-based-insurance-surcharges-canada/#:~:text=The%20IntelliDrive%20app%20by%20Travelers,regular%20premium%20through%20safe%20driving

Notion Data Leak

Strac offers a Data Leak Prevention (DLP) solution for Notion, a productivity app, to ensure compliance with HIPAA and safeguard against insider threats. This DLP software detects and redacts sensitive data from Notion's pages, blocks, and comments, focusing on PII or PHI data. Businesses can configure specific data elements for redaction, and compliance officers receive audit reports on data access. Strac's technology is designed to protect sensitive information within Notion by masking it, thereby supporting regulatory compliance and minimizing the risk of data leaks through advanced detection and redaction capabilities.

Reference: https://www.strac.io/integrations/notion-dlp