**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



# Social Media and Data: How are Social Media Companies Collecting and Using Your Personal and Corporate Data?

Tom Andrews

**Tom Andrews**
Founder and CEO
Rightly

***Biography***

*Tom Andrews is the Founder and CEO at Rightly (https://www.rightly.co.uk). In 2018, Tom founded Rightly because he saw an opportunity to use the new consumer legislation and protection on personal data to help people understand what's happening to their data – and take control of it. Launching in May 2020, Rightly has already helped over 60,000 people and works with 12,000 firms.*

*Attending university at Imperial College, London, Tom graduated with a Bachelor of Science (BSc) in Physics. He has always been analytically minded and after university he followed a career in problems solving for businesses like KPMG and PwC, focused on financial markets, risk assurance and forensic accountancy.*

**Keywords** Privacy policies, Data breaches, Personal data, General Data Protection Regulations (GDPR), Micro-targeting campaigns, Political misinformation, Social media, Rightly
**Paper type** Research

## Abstract

*Social media companies have developed an increasingly bad reputation for how they handle the personal data of their users. With privacy policies on social media platforms being so notoriously hard and labour-intensive to read, making it difficult for users to quickly find out about themselves, the author of this article explains exactly what some of the World's biggest social media companies are actually doing with our data.*

## Introduction – Why has Cambridge Analytica changed our perception of personal data?

The Cambridge Analytica scandal changed all our perceptions of 'personal data' for all time, and with documentaries such as Netflix's *The Social Dilemma* making data accessible, it is easy to see why more and more people are concerned about their privacy. In 2018, the Cambridge Analytica scandal saw personal data as a concept entering public consciousness, but it was being mined and misused through apps to influence people's decisions long before that: from your choice of pet food to political party. Back in 2010, Facebook launched 'Open Graph', a platform that enables external developers to reach Facebook users and their personal data – as well as the personal data of their friends – through mobile apps.


**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



This enabled the mass collection of personal data, which eventually led to Cambridge Analytica, a political consulting firm, to collect vast amounts of personal information and use it to attempt to sway voters. They were eventually exposed, and given a huge fine of $5 billion by the Federal Trade Commission.

Britain's Information Commissioner seized Cambridge Analytica's servers, and 73 external experts were called to answer 4,350 questions from MPs in the UK Parliament's investigation – and the value of Facebook shares plummeted.

Yet, the social media behemoth did not fully co-operate on home soil or in the UK, leading Jason Kent, the chief executive of Digital Content Next to declare that "Facebook is not just bigger than any nation state on Earth, with 1.74 billion users and plays a pivotal role in their elections, but that it's completely out of control". The UK Parliament's final report was in keeping with this sentiment, stating that beyond not co-operating, Facebook had treated the Parliament's investigation with 'contempt'.

When Mark Zuckerberg was questioned by U.S. Representative Alexandria Ocasio Cortez a year later, he admitted that he didn't know at what point his company became aware of Cambridge Analytica's operations, to which she said: "This was the largest data scandal with respect to your company, that had catastrophic impacts on the 2016 election. You don't – you don't know?"

The UK Information Commissioner then issued Facebook with their maximum fine of £500,000, and warned that 'democracy is under threat', and called for an 'ethical pause' on micro-targeting political ad campaigns.

In America, alongside ordering Facebook to pay a record-breaking $5 billion penalty, the Federal Trade Commission enforced new restrictions on Facebook, and a modified corporate structure, that aims to hold them accountable for decisions made that affect the privacy of their users.

## So why are we still talking about Cambridge Analytica and data theft all these years on?

According to Forbes, and Facebook itself, it's still happening. A year later after the scandal broke, Facebook admitted that roughly 100 developers may have improperly accessed user data. This means that revelations about Cambridge Analytica only exposed one small fraction of what is, in reality, an entire data market largely out of the reach of regulatory authorities.

Today, society's relationship with data has permanently changed. Cambridge Analytica has been shut down, and 'personal data' isn't such a strange term to hear in everyday conversation. We have become accustomed to requests about our data when we visit websites, and being asked to click 'accept', or 'adjust' or 'deny' on pop-up privacy settings.

However, in an age of micro-targeting and widespread political misinformation, we need to understand how our data is being used before we click 'accept', know where it is being stored, and how to get it back.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**




So let's look at the privacy policy of some of the world's biggest social media companies.

## Facebook's privacy policy – What data do they collect about you?

Facebook collects various kinds of information about you. Some examples include:

- Personal information used to create an account;
- Information in content you upload like location or photo information;
- Information in content other people upload about you;
- How you use the site, what you engage with, and who you talk to;
- Transactions through Facebook, such as in games or through Marketplace;
- Device information like IP address, operating system, and network data;
- Information from third-parties who use Facebook features such as the like button or Facebook pixel.

### Do they share your data with third-parties for advertising purposes?

Yes. While Facebook makes it clear that they "don't sell any of your information to anyone and [...] never will", they do share information with partners in various ways.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**




Facebook doesn't share data that personally identifies you without permission, but it does share demographic info with advertisers to let them know how their ads are performing.

## Who with?

Facebook lists some of the kinds of people they share your information with, including:

- Advertisers;
- Data measurement companies;
- Vendors and service providers;
- Researchers and academics;
- Law enforcement.

## Any headlines?

The Cambridge Analytica scandal[1] in 2018 is currently the most famous that saw millions of Facebook users' personal information gathered and sold without consent. An app created by a Cambridge academic was used to collect data such as public profile, page likes, birthday, and location, which was then used to create individualized profiles. Suggestions for political advertisements were attached to each profile, and then the information was sold to political campaigns. The 2016 campaign teams of Ted Cruz and Donald Trump both purchased data, and speculation surrounds whether the UK's Leave campaign also bought in.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**




## Instagram's privacy policy – What do they collect about you?

Acquired by Facebook in 2012, Instagram shares a lot of its parent company's privacy policies.

Instagram collects various kinds of information about you. Not all data is shared with third parties. Some examples include:

- Personal information used to create an account;
- Information in content you upload like location or photo information;
- Information in content other people upload about you;
- How you use the site, what you engage with, and who you talk to;
- Transactions through Instagram;
- Device information like IP address, operating system, and network data;
- Information from third-parties who use Facebook features such as the share to Instagram button or Facebook pixel.

### Do they share your data with third-parties for advertising purposes?

Yes. Like its parent company, Instagram makes it clear that they "don't sell any of your information to anyone and [...] never will", they do share information with partners in various ways. Facebook doesn't share data that personally identifies you without permission, but it does share demographic info with advertisers to let them know how their ads are performing.


**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



## Who with?

Instagram lists some of the kinds of people they share your information with, but they specify that this info is rarely personally identifying. These companies include:

- Advertisers;
- Data measurement companies;
- Vendors and service providers;
- Researchers and academics;
- Law enforcement.

## Any headlines?

A significant data breach in August 2020 affected a number of social media companies and their users. The security research team at Comparitech disclosed how an unsecured database left almost 235 million Instagram, TikTok and YouTube user profiles exposed online in what can only be described as a massive data leak[2].


## Twitter's privacy policy – what data do they collect about you?

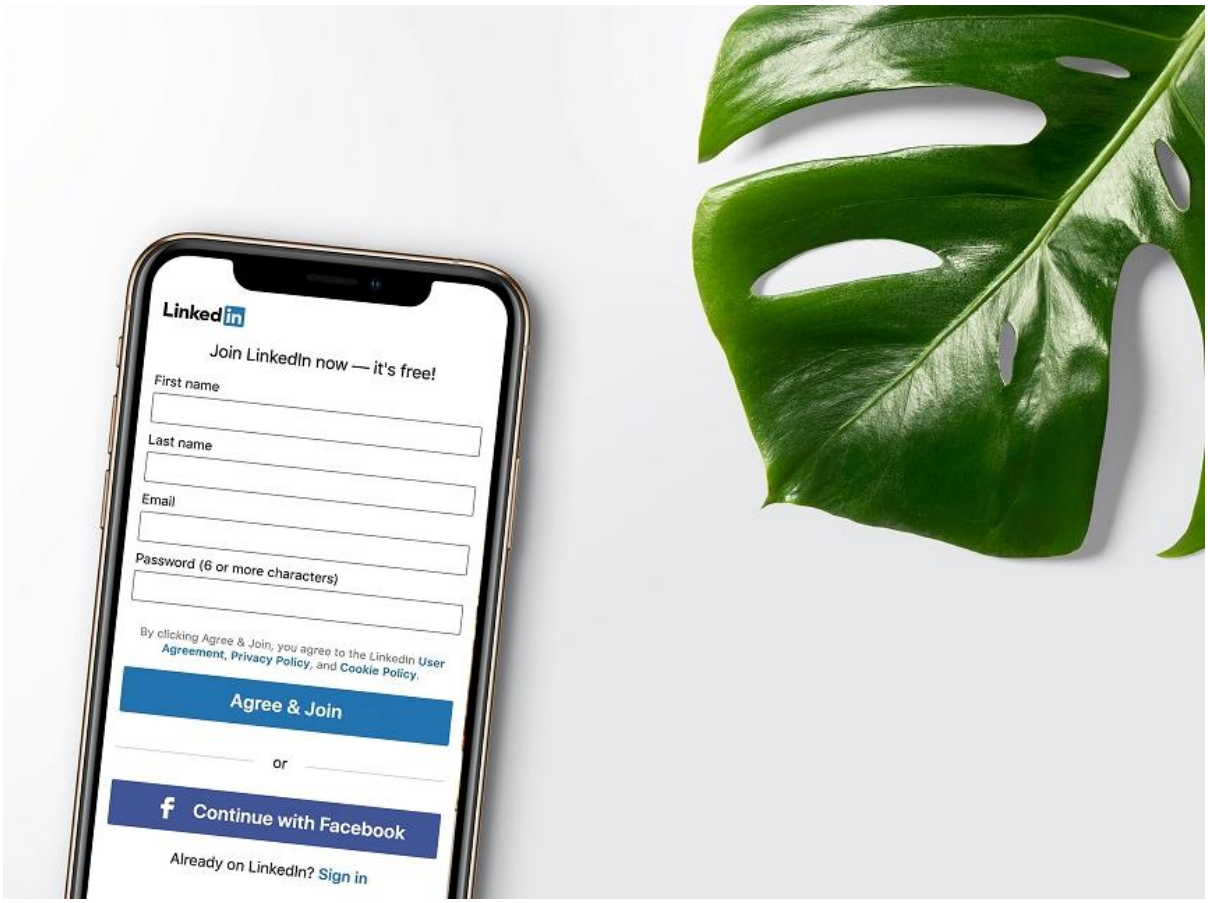
Twitter collects various kinds of information about you. Not all data is shared with third parties. Some examples include:

- Personal info used to create an account;
- Payment information if paid services are used.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**






## LinkedIn's privacy policy – what data do they collect about you?

We all use LinkedIn in business, so LinkedIn collects a number of different types of data, such as:

- Name, email, mobile number, and sometimes payment info;
- Email header information if email accounts are synched;
- Personal profile information such as education or work;
- Synced contacts or calendar events;
- Information collected through third-parties who use LinkedIn's services.

### Do they share your data with third-parties for advertising purposes?

Yes. LinkedIn serve tailored ads on their site and elsewhere on the web, and share some data with third parties in connection with those services. The company shares certain information with advertising providers, such as how an ad is performing, device identifiers, and profile data.

While LinkedIn states that "do not share your personal data with any third-party" (excluding the kinds listed above), they do note that if you view an ad through their platform, advertisers can "determine it is you" through cookie identifiers and other technologies. In these cases, LinkedIn "contractually require such advertising partners to obtain your explicit, opt-in consent before doing so."


**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



## Do they share your data with third-parties for advertising purposes?

Yes. Twitter shares user information with third-parties, but usually only shares non-personal, aggregated information to let advertisers know how their ads are performing. This kind of information includes demographics, engagement such as clicks or votes on polls, inferred interests, or location. However, Twitter's ad policy prohibits companies from "targeting ads based on categories that [they] consider sensitive or are prohibited by law, such as race, religion, politics, sex life, or health."

## Who with?

Twitter shares info with third-parties from a number of areas:

- Advertisers;
- "Service providers" such as Google Analytics or payment companies;
- Law enforcement.

## Any headlines?

In June 2020 Twitter contacted business clients[3] who used Twitter's advertising and analytics platforms to inform them that personal information might have been compromised. The scale of the breach wasn't clear. In 2018, 330 million users were similarly contacted[4] and urged to change their passwords after some were exposed.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



## Who with?

LinkedIn shares this kind of personal information with areas such as:

- Advertisers;
- "Affiliated entities", including all other Microsoft platforms;
- Law enforcement agencies.

## Any headlines?

In 2016 LinkedIn discovered a 2012 hack[5] of the company which exposed up to 165 million user passwords. More recently in January 2020 LinkedIn's parent company Microsoft was shown to have been hacked[6], exposing 250 million customer records online. Whether this included specific LinkedIn-related information is unclear, but it doesn't bode well for the social platform's security.


## YouTube's privacy policy – what data do they collect about you?

YouTube's data collection practices fall under its parent company Google who collects a variety of personal information, including:

- Name, email, and sometimes phone number and payment information;
- Search history;
- Purchases;
- Interaction with ads and content;
- Location through device information.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.
The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



## Do they share your data with third-parties for advertising purposes?

Yes. Google (and YouTube) uses personal information to customize advertising services. Personalized ads are based on interests, and some information is shared with advertisers. Google doesn't show personalized ads based on sensitive categories "such as race, religion, sexual orientation, or health", and doesn't share personally identifying information such as name or email. However, as with LinkedIn, if you engage with an advertisement the advertiser can use cookies to personally identify you later.

## Who with?

Google shares personal data with a number of categories, such as:

- Google "affiliates", meaning their entire suite of companies;
- "Over 2 million non-Google websites" who run ads through Google;
- Law enforcement.

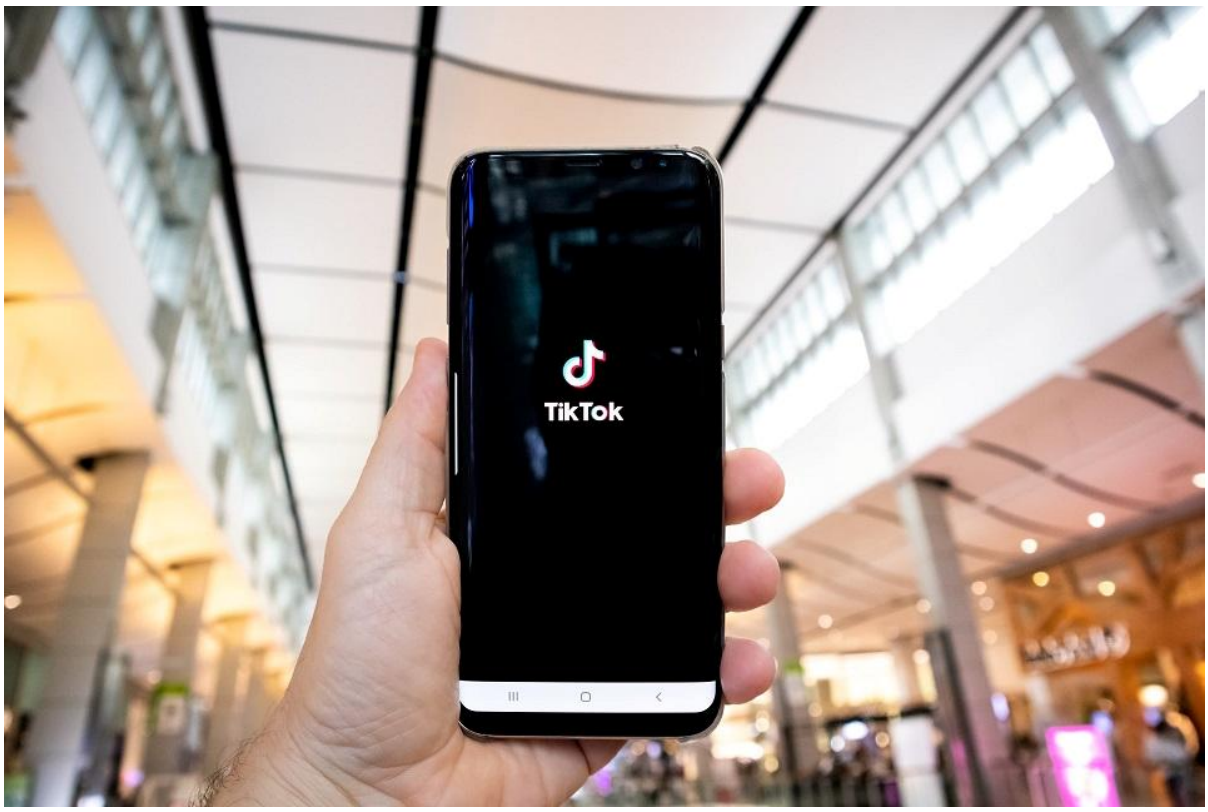
## Any headlines?

In 2018 Google discovered a leakage in their social platform Google+ which led to the compromising of over 5 million users' data[7]. An additional bug in the service subsequently led to the exposure of user data from a further 52.5 million accounts[8]. The leaks went unreported until the Wall Street Journal broke the story, prompting Google to eventually shut down Google+ in 2019.

**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**






## TikTok's privacy policy – what data do they collect about you?

TikTok collects a really significant amount of personal data, including:

- Age, username and password;
- Phone number and email;
- Content uploaded by or about you on their platform;
- Interactions on their platform;
- Payment information;
- Synced phone and social network contacts;
- Information from third-parties like other social media platforms;
- Device information and location data.

### Do they share your data with third-parties for advertising purposes?

Yes, TikTok shares some data with third parties. The platform only shares aggregated user information with third-party ad companies, meaning you can't be personally identified by advertisers.

### Who with?

Partners that TikTok shares data with include:

- Business partners like other social networks (Facebook, Twitter etc.);
- Payment providers;
- Service providers and analytics companies;
- Advertisers;


**CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW** is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**



- TikTok's "Corporate Group" (under its parent company ByteDance);
- Law enforcement.

## Any headlines?

TikTok has been a turbulent new contender in the social media industry, and has had its fair share of controversy, particularly due to its popularity with kids. In February 2019 the US Federal Trade Commission fined TikTok a record £4.2 million[9] for illegally collecting personal information from children under 13. Both the UK and the US launched investigations[10] into TikTok's handling of childrens' data and their compliance with GDPR.

## In conclusion

Privacy policies are often unnecessarily confusing and time-consuming to read. At Rightly, we believe it shouldn't have to be that way. Companies should provide a clear, transparent and easily scannable document that tells their users exactly what happens to their personal data. Until that happens with social media companies, hopefully we've made it a little easier for you.

**Reference**

1 https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
2 https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=583bc0121111
3 https://www.bbc.co.uk/news/technology-53150157
4 https://www.bbc.co.uk/news/business-43995168
5 https://www.wired.co.uk/article/linkedin-data-breach-find-out-included
6 https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=695f0ef54d1b
7 https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194
8 https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/
9 https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use
10 https://www.forbes.com/sites/zakdoffman/2019/07/03/tiktok-investigated-for-breaches-of-child-safety-and-privacy-yet-again/?sh=2652c8d92e6f