Handling data is Facebook's biggest source of revenue. In 2016, the company made $6.4 billion in advertising, marking a 63% rise from the previous year.

Few people realise the exact extent to which Facebook's data-collecting machinery operates. In addition to processing profile information, Facebook tracks you offsite and buy information about your offline activity from third parties. Thanks to the combined power of these sources, Facebook is able to develop consumer profiles so detailed that it can raise privacy concerns.

What Data Is Collected

Facebook's data use policy (last revised on September 29, 2016) states the types of information it collects about you. Some of it is collected onsite and some offsite.

1. Onsite data:

Everything you share on Facebook, including your account details, the posts you publish, the location and dates of photos, the ways you use Facebook (such as what type of content you engage with, how frequently, who you communicate with).

Everything others publish about you, including photos, messages, and posts.

The groups and people you are connected with, including data on how you interact with them and contact information (for instance, an address book) you upload.

Payments information, such as what type of purchase or donation you made, your card information (card number, card security code and so on) as well as contact, billing, and shipping details.

2. Offsite data:

All pieces of information about your device, such as operating system, hardware version, device settings, file and software names and types, battery and signal strength, device identifiers, specific locations gathered via GPS, Bluetooth or WiFi, the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

Information from third-party websites and apps associated with Facebook, such as games on Facebook. The information includes what websites and apps you visit.

Information supplied by third-party partners, such as advertisers or

data brokers.
Information supplied by other companies owned by Facebook.

How Data Is Collected

Some data gathering techniques, such as simply saving your account details or Facebook activity log, are obvious. Others are not that clear. In 2015, Facebook lost a case in Belgian court, which related to Facebook's data collection. A team of researchers from the Universities of Leuven and Brussels concluded that every time a person visited a Facebook page or a website with a Facebook like button, a cookie called datr was stored secretly on the browser—even on the browsers of non-users. The cookie was designed to live two years and track all browsing activity. The court decided that collecting information on non-users without their consent was against EU law. In 2016, Facebook won an appeal on the grounds that Facebook, whose European headquarters are in Ireland, cannot be judged under Belgian jurisdiction. So as of now, Facebook is free to track its members and non-members.
To make its consumer profiling even more detailed, Facebook buys information on your online and offline behaviour from third parties.

Facebook and Third-Party Data Brokers

Data collecting is a gigantic industry operating in the shadows. Data brokers are companies that collect and analyse publicly available data to build detailed consumer profiles. Their dossiers may contain such information as whether you own a dog, what your favourite brand of tea is, the size of your shoes, whether you're pregnant, and your credit card habits. According to the New York Times Acxiom, one of the biggest data brokers in the world, categorizes consumers into such sensitive groups as "potential inheritor", "adult with senior parent", "diabetic focus", "dieting", "gaming-casino", "money seeking", and "smoking-tobacco".

How do data brokers collect information about you? They obtain it from government open data (for instance, if you made a political donation), publicly available data (your social media profiles), and commercial data (your purchases). Any consumer contests, surveys, warranties, loyalty card purchases or magazine subscription lists are taken into account. This data feeds complicated algorithms, which categorize you into thousands of targetable categories.
Data collection is especially widespread in the US, where data protection

laws are inadequate. Data brokers are not even lawfully obliged to show you the information dossier they have about you. Even if they decide to do it for the sake of “transparency”, they can cherry-pick or make the process of accessing information ridiculously burdensome.

To give you an idea of the scope of the data collecting industry, the firm Datalogix, (which was the first data broker Facebook signed an agreement with in 2012) has information on nearly every household in the US and $1 trillion in consumer transactions. Acxiom, another data broker associated with Facebook, has information on about 500 million consumers in the whole world with about 1,500 data points per person.

Facebook’s advertising categories provided by third parties are usually financial ones, such as your approximate household income, value of your assets, or whether you go to low-cost shops.

How Your Data Is Used

Data is used to provide services, such as making content suggestions, helping you find a local event, or displaying news tailored to your preferences.

Information is also shared with all platforms and applications owned by Facebook (look at the “What Data Is Collected” section of this article for a full list of these platforms).

Lastly, Facebook uses your data to provide marketing services. As the Facebook use of data policy page states: “With this in mind, we use all of the information we have about you to show you relevant ads.”

Facebook doesn’t share personally identifiable information (which is information that could identify you by name or suffice to contact you — such as your name or email address). However, it shares *all* other types of information, including your interests, browsing history, location, payments information, groups, relationship status, family information, everything others publish about you, etc.

Profiling and its Dangers

Is using your data for marketing purposes really a problem? After all, Facebook doesn’t share so-called personally identifiable information. Few businesses could exist today if they weren’t able to target the right

audiences. Besides, some consumers consider it a convenience to have ads tailored to their needs.

Everything depends on the scale. Peter Eckersley, the chief computer scientist at the Electronic Frontiers, says that even if companies normally use some of Facebook's methods of gathering information, no company uses all of them at once.

Some advertising categories offered by Facebook may also raise concern. Here are some examples: age, location, square footage of home, ethnic information, the year in which your home was built, users who are away from home, users who are newly married, your political opinions, your employer, users who want to buy a new car (with all the details such as the brand, colour, and so on), how many employees your company has, users who invest, your credit type card, users who listen to the radio, users who use coupons, users who buy medications and what kind of medications, types of restaurants you eat at, users who own motorcycles, and thousands more.

Apart from the obvious worry that so much information is focused at one company (consider that Facebook has 1.94 billion monthly active users as of 2017, over a quarter of Earth's population), data may be abused by advertisers in quite palpable ways. For instance, owners of motorcycles may be offered insurance coverage at higher prices. Or low-income people may be offered low-quality mortgages offers.

Can You Opt-Out?

The short answer is no.

The long answer is it depends on what you want to opt out of. You can opt out of having targeted advertisement shown to you—which, however, doesn't mean that Facebook isn't spying you anymore. Telling data brokers to stop collecting your data, although in theory possible, in practice is an insurmountable task. To opt out of Datalogix, you need to send a written request with a copy of your ID. Julia Angwin, the author of *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* tried to opt out of as many as 92 data brokers that had an opt-out option. In the end, it proved impossible in the majority of cases.

There are some ways to reduce the damage. You can change your privacy settings to decide who can see your posts and profile information.

You can install Tor, which is a software that will make you anonymous on the Internet.

However, the only definite way of stopping Facebook from collecting your information is by deleting your account. As the data use policy states: “We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.”

This presents a real problem for a majority of people. I, for once, know that I would lose some of the friendships I’ve made over the years with people from all over the world. Facebook is so convenient precisely because everyone uses it. But this also gives the company the power to do as it will with our personal data.