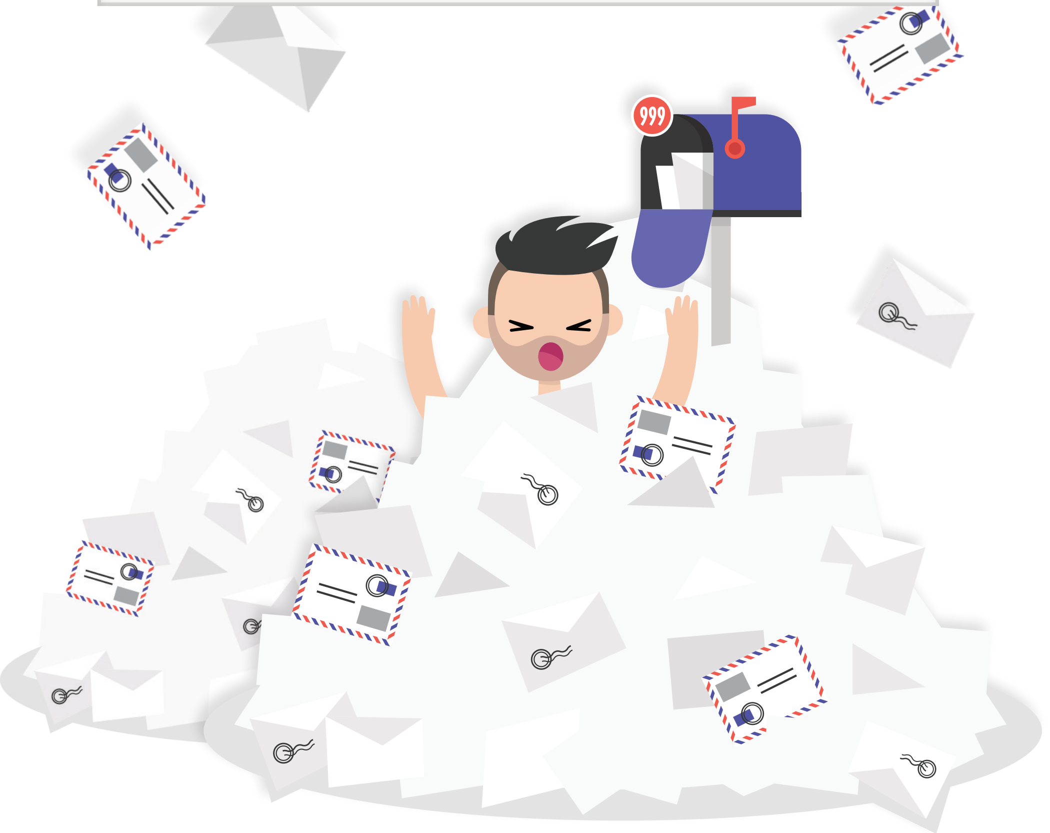
How Brands Use Your Info After Sign-ups

And What You Can Do About It



In April of 2019, Business Insider reported that Facebook had harvested the email contacts of 1.5 million users without user consent upon the opening of their accounts. Facebook claims to have done this in order to improve its targeted ads, and claims the contacts were uploaded to Facebook unintentionally. This comes on the wake of a difficult time for the trust relationship between the social media giant and its users, and it reinforces, once again, the ever-growing need for a stronger focus on information privacy.

Every day, millions of Americans freely give out their email addresses and phone numbers to services, subscriptions, social media platforms, surveys, wi-fi networks, and more. This information is recorded and used for targeted marketing campaigns, tracking, and is a sold commodity fueling an industry of data-brokers who buy and sell the personal information of strangers. According to the Open Society Foundation, this industry generated $156 billion in revenue in 2012.

While much of this activity happens behind closed doors and remains undercover, the vast majority of information transaction is kick-started by the consent of consumers who don't read the terms and conditions, don't interact with privacy policies, or are simply used to the idea of sharing information for access to basic services.

This resource was developed to help educate and contribute to the growing conversation surrounding awareness of online privacy issues. It covers the ways in which companies gather your information, what happens to that info once they have it, and ways in which you can protect yourself while still having access to online resources, services, and more.

Our Consent is The Gateway

A person who truly engages with the terms of service, conditions, and privacy policy related to a service, subscription, or social media platform is a rare find. Often, we find that we lack the time, patience, or understanding required to sift through one of these digital contracts, simply clicking "I agree" and ignoring that voice in our conscious that reminds us of the danger we agreed to.

If the average American took the necessary time to read through each of their agreed upon digital contracts, it could take up to 250 hours per year. Along with this, many of these contracts are intentionally front-loaded with legal jargon and word smithing that makes them difficult to unpack and truly understand. An article from the New York Times put Facebook's privacy policy on par with works of literature that require at least a college reading level. Hulu's privacy policy was listed as more difficult to read than Immanuel Kant's Critique of Pure Reason.

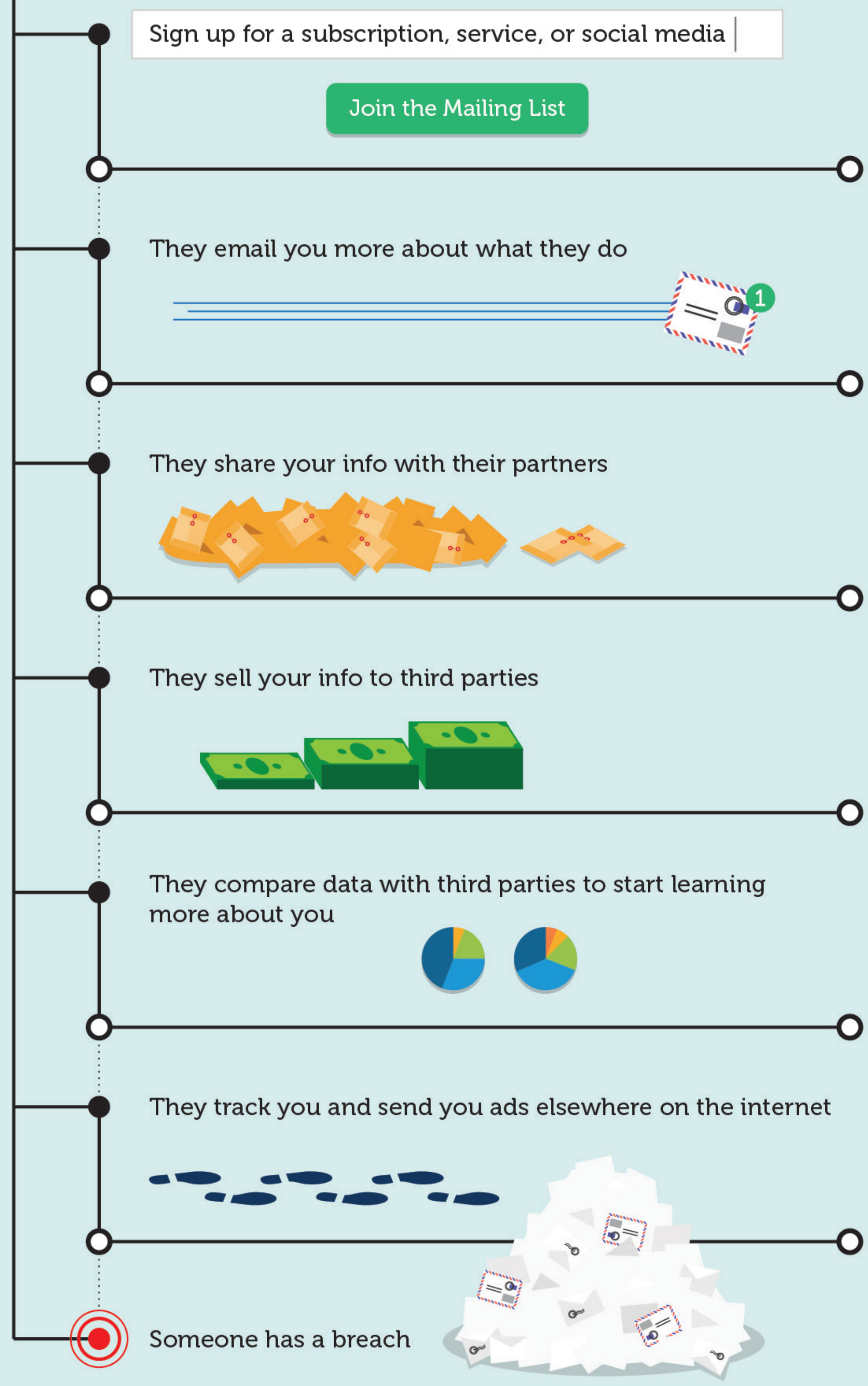
The stipulations hidden within are as bad as you may think. For example, in order to use Spotify, the music streaming service reserves the right to "collect information stored on your mobile device, such as contacts, photos, or media files." For Facebook, they maintain the ability to keep your photos and content even after your account is deleted, and Netflix, along with a number of others, have the right to disclose your info to 3rd parties when they deem it necessary.

So what happens to your info once these companies have it? Sometimes, depending on the nature of the product and the underlying goals of a brand, not much. But in many cases, a domino effect with a few varying degrees of results could ensue.

First, you are sent content related to whatever form you filled out to use the service or subscription. This was to be expected. You may receive suggestions on how to use the service or notifications in your inbox. No big deal! That said, with so many services so interconnected, your info is then susceptible to be used in tandem with other brands. For example, since Instagram is owned by Facebook, you'll often find the content you're presented to be similar, and their ads will retarget you across platforms. You may also see this reflected in your inbox.

From here, the next step is a sale of your information. Facebook has been under fire as this aspect of their marketing initiatives have come to light in recent years, after selling messages, demographics, and interests found from watching their users. Along with this, data-brokers will sell email addresses and phone numbers to third party vendors in order for this info to be added to email marketing lists. A common way this happens is through promotional giveaways.

How Your Info Travels on the Web



Sign up for a subscription, service, or social media

They email you more about what they do

They share your info with their partners

They sell your info to third parties

They compare data with third parties to start learning more about you

They track you and send you ads elsewhere on the internet

Someone has a breach

Now that these companies have you settled into a certain demographic, they begin comparing traits from following you with others like you in order to learn more. This comes closely with being advertised certain products and opportunities that pertain to you on sites you may have never been to before.

Of course, the worst case scenario of all is a data breach. According to Risk Based Security, over 6,500 publicly disclosed breaches occurred in 2018 worldwide, resulting in 5 billion exposed records. Many of these breaches, both in 2018 and in the 21st century as a whole, occurred in high profile companies, such as Target, Marriott, and the PlayStation Network.

What You Can Do

There are plenty of practical tips and tools you can use in order to help maintain your privacy online, including browser and phone settings, personal information best practices, and downloadable add-ons.

Of course, the best way to protect your info from being sold, leaked, or otherwise misused for marketing is to never sign up for things, which isn't our most practical piece of advice since so much important activity happens online. Rather, an excellent place to start may be to use an alternate email address strictly for signups. This will prevent marketing spam mail traced from signups using your email from interfering with your primary email account. That said, this is more difficult to apply to a phone number, as many do not have the patience or resources to open another phone number just to use at signups.

Much of our collective lack of privacy happens from location services in apps. Often, an app like SnapChat or Google Maps will request access to your location in order to better utilize its features. However, this location tracking isn't always turned off once users close out of the app. The result is a very efficient system for tracking locations of individual users for companies, and sometimes even other people. Turning off location services unless it is absolutely necessary to use lets you win back location privacy from your phone.

Along with these practical tips, there are a number of applications, add-ons, and special tools you can use to prevent tracking. One such tool that is very popular, both for its usability and its privacy resources, is Duck Duck Go. As a search engine alternative to Google and Yahoo, Duck Duck Go allows you to surf the web without having your search history and interests tracked.

Our very own ID Incognito is also incredibly useful as our way of safeguarding your email address and phone number at signups. ID Incognito works by providing alternate email addresses and phone numbers (we call them personal information aliases) to users for use instead of real contact info when signing up for things online. If a service or subscription needs to send them a confirmation code or newsletter, users can have this content forwarded to them and even respond. But companies never see their real info. This means no spam calls or marketing emails sent to your inbox. It's all filtered through us.

Another useful tool is Tor, an alternative browser that automatically encrypts your data 3 times as you use it. This means that each individual user looks generic in the eyes of network trackers, which allows you to search and engage with content without being traced across the web.

Whether you find yourself concerned for your privacy on a threatening level, or simply grow tired of the idea of marketers having your info, establishing online privacy is not out of reach. The Internet is dangerous and full of agendas that don't include consideration of your privacy, but you can fight back with plenty of helpful tips and tools in mind. And, while the Internet demands be taken one site at a time, we hope you find that, with a little knowledge of the way information travels, privacy can be practical.

Thank you for downloading this resource!

If you're interested in an ID Incognito personal information alias, please follow this link: www.idincognito.com and let that be the last time you ever give out your personal email or phone numxber on the web!