- Social networking

ARE YOU TOO EXPOSED ONFACEBOOK?

Even if you've never used an app, or never signed up for Facebook, you've appeared in the contacts of people who did

Philippine Daily Inquirer · 29 Apr 2018 · A1 · By Lou Gonzales @Inq_Lifestyle

How big of a digital footprint do you leave behind? You're likely a Bigfoot in the digital sphere, and Facebook is not to be blamed— not entirely anyway.

You've probably been bombarded with the Facebook/Cambridge Analytica scandal the past couple of weeks, and have seen videos of Mark Zuckerberg's appearance before the United States Senate. Either that, or you've been ignoring it.

However, it should be your concern, simply because you're using the internet.

What happened with Facebook and Cambridge Analytica that led to a US Senate inquiry? In a nutshell, if you used an app on Facebook called "This is your digital life," chances are, Cambridge Analytica may have harvested your details, along with your friends' details, and used them for a political campaign. Facebook's disclosure suggested that Cambridge Analytica improperly obtained user data that could have given it an unfair advantage in reaching voters. It's troubling, right? Unfortunately, it doesn't end there.

'Shadow profiles'

Even if you've never used an app, or never signed up for Facebook, you've appeared in the contacts of people who did. This is how you have "recommended friends" or "people you may know" suggestions on social media. When users connect their e-mail account or texting data with Facebook, countless nonusers are swept up. Facebook allegedly keeps these nonuser data, called "shadow profile," so that when nonusers sign up on Facebook, the company will know exactly who to recommend as friends.

On almost every website, we see Facebook "like" or "share" buttons. You have trackers all over the web. It doesn't matter if you have an account or not—Facebook is able to collect information from all of us.

And, as if that's not troubling enough, it's not only Facebook that collects our information. I went on a social media "boot camp" at Google's Mountainview headquarters years ago, back when social media was just start- ing. Google told us that its social media marketing app is designed to target individuals precisely based on their interests, geographical location, etc.

Our trainer said, "For example, I want to target 1,000 Lou Gonzaleses on Facebook, this app can do that for you." Since I've never heard of anything like that at the time, I said, "Wow, that's creepy." And they said, "It does sound creepy, right? But it's really only based on what you put out there."

So, they can target 1,000 other divers and foodies and travelers because these are the things I repost, comment on, share.

Data collection

The idea that you can target marketing messages based on individual psy- chographic profiles, and the surreptitious collection of data under the guise of market research, later used to promote a campaign—does this sound new to you? It seems like a legit marketing tactic that has been used long before social media.

Perhaps we just didn't grasp the implications, until news came out the consequence may have been the election of Donald Trump, or the emergence of DDS (Diehard Duterte Supporter) trolls.

If Facebook's access to psychographic data was known to many marketers, so was the tactic of disguising data collection as fun games and quizzes. Admit it, weren't you the least bit curious what type of personality you have? Or your level of OCD? Or your expertise in pronouncing the names of French dishes?

But you should know that marketers really mean well. The purpose of collecting data is to ensure that brands can make better decisions about which content they should promote to you. Cambridge Analytica was hardly an outlier there, either. To marketers, it was normal to harvest
data and use it to target individual ads, long before this company got in on the action.

There's a difference between actually representing what your services are and how they can help people, as opposed to sway people with fake news. Unfortunately, there's always the latter when marketers can take advantage of your data.

Simple steps

Here are some simple steps to not give away everything.

Know what you are sharing. For starters, you can see all the pertinent information related to your account by downloading your Facebook archive. This includes your photos, chat history, IP addresses, active sessions, which ads you clicked and basically all the things you did on the internet—including facial recognition if, at some point, you became curious about how your future child will look like, for instance. To download your archive, go to "Settings" and click "Download a copy of your Facebook data" at the bottom of General Account Settings, and then click "Start My Archive."

Disable data tracking and location services.

Next, keep your information private by disabling data tracking and collection. Location service is the most sensitive data you can grant to any third-party or service. Turn off your location services on your smart phone. It makes sense to grant Google maps and Waze access to your location; otherwise, just turn it off for the other apps. For iOS users, you have the option to allow Facebook or any other apps to use your location "always," "while using the App," or "Never."

Purge your apps. Remove the apps you no longer use, or you never knew you actually used. Head over to "Settings" and go to "Apps and websites." At this writing, I had 110 apps over the years, but have kept only 20 active ones. I just recently removed Quizztar, Kuezz and all the other quizzes I've taken. I was gullible like that, too! If you're extra paranoid, scroll down to the bottom of the page to "Apps, websites, games," and turn off the ability to interact with any apps entirely.

Limit your share settings and customize your ad profile.

Limit your share settings. You have options to share your posts privately—to your friends only, to friends of friends, or to the world. It is entirely up to you.

Most importantly, restrict your ad settings by removing categories that you don't want advertisers to reach you for. Go to facebook.com/ads/ preferences.

It has categories such as your interests, advertisers you've interacted with and your personal information. You will be surprised at the wealth of information Facebook has on you, based on what you put out there and what types of ads you clicked on. They know the network type and browser I use, what computer and phone I use, down to its operating system. They know my interests, from business and industry to news and entertainment, hobbies and activities, food and drink, shopping and fashion and more. I'd hate to think they know me more than I know myself!

It's time for us to face up to what marketers and researchers have known way before the internet: marketing runs on the knowledge and analysis of user data, and that won't change. In fact, it has evolved to maximize the amount of data collected and the precision of ad targeting.

So, if you don't feel comfortable about other people using your data, at the very least, be aware of the data that you do put out there.