Handle Your Data Like a Privacy Professional

Author : Cat

Date : January 24, 2021

Whenever I visit a specialist, like a car mechanic or a dentist, and they give me options, I always ask "what would YOU do in this situation?" I like to defer to the professional's opinion. Why not apply this to privacy?

I reached out to my network of privacy consultants, lawyers, and security specialists and asked 20 respected Privacy Professionals from around the globe the same five privacy questions:

1. What application or service you will NOT install on your phone?
2. What application or service do you know takes your data but the value of that application is worth it anyway?
3. What piece of data do you wish people would stop sharing?
4. What's your favourite book or movie about privacy?
5. Admittedly, do you have at least one password that is your pet's name?

1. What application or service you will NOT install on your phone?

Not surprisingly, the number one answer here was Facebook. It takes too much data and their privacy practices have not shown to be in the best interest of the individuals. The experts agreed that any app whose financial model is to earn money off user data is a no-go for them. Second is TikTok as it acts as spyware and does not follow the same privacy rules as regulated countries. Other answers fell around uncertified websites, anti-virus (as it combs your computer), banking, and any app or service that does not properly lay out their data use in their privacy policy.

Though my own answer was TikTok, I could also add gig-economy apps for services like Uber and food delivery. These should be carefully considered as they not only collect location data and preferences, but that data gets passed down to individuals who may not value your privacy. All of these options should be weighed before you hand over your data.

2. What application or service do you know takes your data but the value of that application is worth it anyway?

We live in a digital world which means there are inevitably some apps we need to use. My vote went to the suite of Google Apps, which is the highest answer. From Gmail, Google Search, Chrome, Android, and YouTube, the alphabet company probably has the most detailed version of your personal data, but the tools are so valuable they are hard to give up. Second in this category was LinkedIn which is key for many for business. The experts who put Facebook and WhatApp here did so begrudgingly because it is the tool of choice for family and/or business contacts. And finally Zoom, a fitness tracker, and a location finding tool.

I sometimes look at this like walking into a room with your skirt tucked into your underwear or your fly down. Have you given away more than you meant to? Maybe. But once people have that information then the damage is done, so why not stay - though you may want limit your data going forward. As an example, I am a long time Facebook user which means they have my data already, but now I am extremely careful about what I interact with and I don't comment on public posts. Use the services and apps you need, but be aware of the data tradeoff in doing so.

3. What piece of data do you wish people would stop sharing?

The answer for this one should really be "all of the above". Tops was kids data. This is threefold; You are defining kids online identities for them, you are sharing their personal information without consent (and modelling that behaviour), and you are putting them at risk for social engineering and data abuse (credit theft is very popular with kids' birthdates and full names). Other risky data includes any kind of personal events and information including your address, names of family members, and location data (watch out for running or biking routes that are routine for you). Also, please share travel plans *after* the trip and not before you have left. Of course the highest risk data are unique identifiers such as your social security, drivers license, and passport numbers. Share these with apps and services only when absolutely necessary.

Last, but not least, data and images should not be shared without consent. And that goes for the applications that share them as well as the people who post them. Be aware of the people in the background of images and videos that you share.

4. What's your favourite book or movie about privacy?

This answer was my favourite because it was a mix of academic research, movies that pull back the curtain on social media, and some sheer entertainment. Half the exerts recommended one or both of the documentaries on Netflix having to do with social media and shared data:

- The Great Hack (2019)
- The Social Dilemma (2020)

Nonfiction books on privacy:

- The Age of Surveillance Capitalism by Shoshana Zuboff
- Race Against Technology by Ruha Benjamin
- The Future of the Internet by Joseph Zittrain
- Habeas Data: Privacy vs. the Rise of Surveillance Tech by Cyrus Farivar
- The Right to Privacy by Caroline Kennedy and Ellen Alderman

- Future Crimes by Marc Goodman
- When Companies Spy on You by Jeri Freedman
- Privacy Blueprint by Woodrow Hartzog
- The Known Citizen by Sarah E. Igo

Documentaries:

- Don't f**k with Cats (2019) [Disturbing imagery]
- The Power of Privacy (2016)
- Screenagers: Next Chapter (2019)
- Citizenfour (2014)

For fun:

- Antitrust (2001)
- Sneakers (1992)

I am going to add The Circle by Dave Eggers to this list. It is both a fiction book and a movie (book is better, obviously) about a google-like social network that tracks everything you do under the guise of it being helpful to others. Sharing is Caring. It well highlights the invasiveness and abuse of data collection.

5. Admittedly, do you have at least one password that is your pet's name?

Over half the respondents said yes to this question (including myself) BUT they all caveated it with the fact that they always use a multi-digit number and/or character with the name. Not the plain text name itself. Plus, most of the experts use a password manager anyway.

That said, this works fine if your pet happens to be named 5$Gu7sk9!s.

Protecting your privacy is up to you! Pause to consider what you are sharing or 'paying' to use a service. Have fun and stay safe.