WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Data Privacy Part 2: You're Sharing Too Much

Written By Angela P. Doughty, CIPP/US (apd@wardandsmith.com)
April 20, 2022

Ed. Note: This is Part 2 of 2 in a series.

We live in an age where our digital footprint is forever preserved. Even before you think twice about it, your data has been collected and saved.

In fact, in 2020, it was estimated that nearly 2MB of data was generated by individuals worldwide every second, and data comes in many forms. There's personal info like social security numbers or a driver's license and physical data such as health records.

In Part 1 of our series, we explained how businesses can become good stewardesses of personal information. Part 2 outlines general best practices to protect your personal data and make informed decisions on when to share it.

The Cost of Convenience

There is a price for everything. Many companies will often request personal information, such as your email, geographic location, contact list, and even access to your photo album before you can use their services.

There is nothing inherently wrong with sharing this information, especially if it's needed to render services, i.e., weather apps and email. But consumers should take time to weigh the benefits of releasing their information and be wary of apps or services asking for non-relevant information.

Delete and Don't Look Back

Forty is the average number of apps people have installed on their smart devices. However, users typically use just 18 apps, and some unused apps can still collect your personal information.

It's best to go through your smart devices, remove the apps that are no longer useful, and protect your personal data by deleting accounts associated with those services.

Manage Your Privacy

Besides deleting unused apps, each application and browser has different features limiting how and with whom you share information. Managing your privacy setting is a daunting task, but peace of mind is a worthy

reward. So, here are a few important things consumers to focus on first:

- Geolocation Data: The data you share with apps can make a huge difference in the results they provide. Make sure that your geolocation information is only going to those who need it and trustworthy websites/applications when using this sensitive info.
- Contact Data: Email apps and video conferencing tools allow for individuals to automatically sync their existing contacts with the services they're using. Therefore, it is important that you ONLY share this data when trustworthy sources are involved, as we have our own personal contact lists and those in our social networks who might be friends or family members.
- Camera and Photo Data: An individual's photo library is a gold mine for data and should only be accessed by trusted sources. The social media apps want access to this information, but they need your permission first! Know what's going on with any app before giving it full privileges so that no one can get into too much private info like passwords or messages (or both).

Lock it Down

It does not matter how much information is on the internet or how strongly it's encrypted; there is nothing more important than protecting your password. Change it often, and use a unique password for every service you sign up for. Password managers are effective for this purpose, and are also helpful in storing other sensitive information. Using multi-factor authentication, when enabled, has been found to block 99.9 percent of automated attacks.

A United Front

From what is shared by consumers to what is collected by businesses, each is responsible for the risks associated with their data practices. And while data breaches and cyberattacks are inevitable, a united front is they only to mitigate the risks.

--