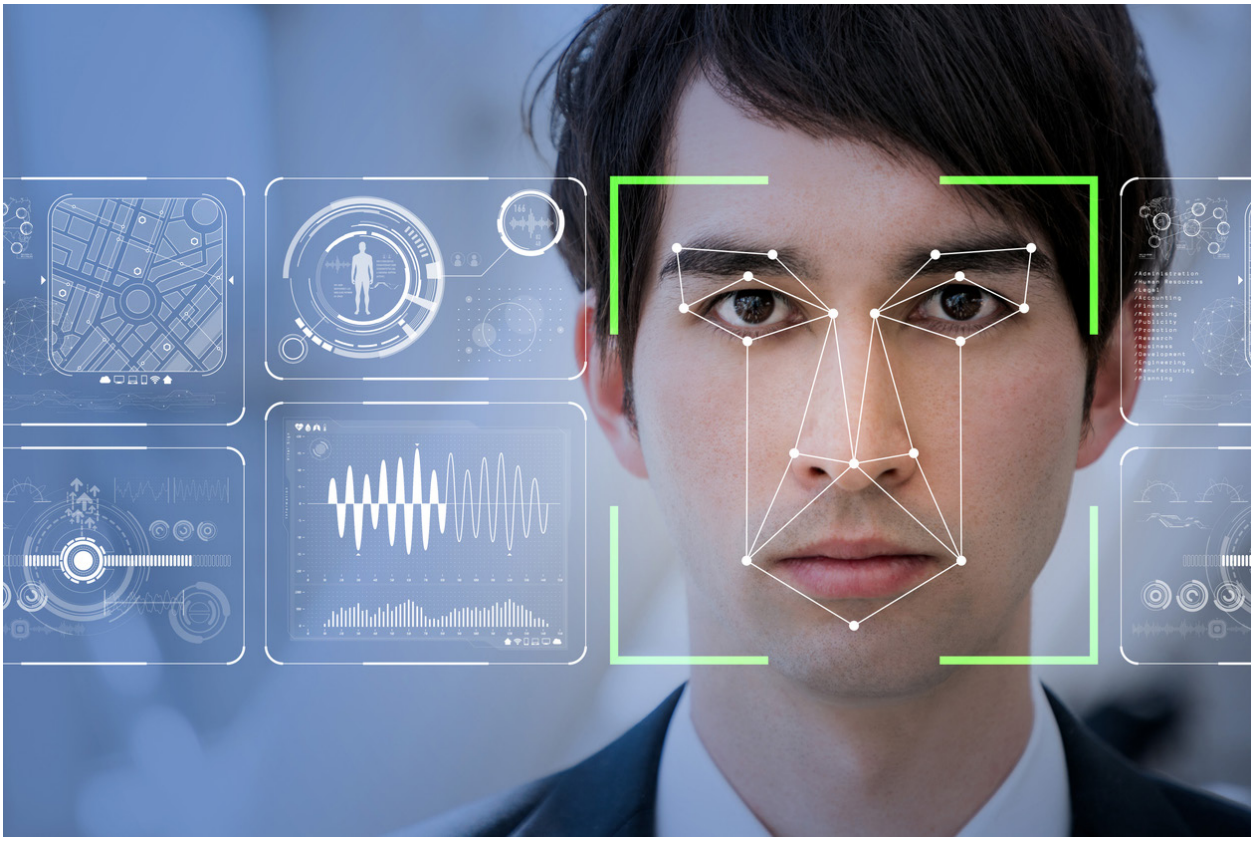
BOSS MAGAZINE

The Cost of Free Apps: Protecting Your Data Privacy in a FaceApp World

By Brian Schrader

The recent FaceApp controversy revealed how easily our private information could end up in the wrong hands. When it comes to free apps, we need to realize that the personal data we're giving away has monetary value.



The photo-filter app FaceApp took the internet by storm earlier this year, with millions of users posting old-age renderings of their faces on social media.

continued next page

But what appeared initially to be a fun online diversion soon raised data privacy concerns as word spread that Wireless Lab, the developer of FaceApp, was based in Russia and that the app's end-user agreement granted the developer wide-ranging access to users' private information.

The full story turned out to be a bit more benign. Although the app's end-user agreement did give the developer greater access to users' private information than was maybe necessary, it certainly didn't go as far as some other widely used software has. Subsequent technical analyses eventually cleared developer Wireless Lab of any suspected mishandling of users' data.

Data privacy is a recurring concern

Looking back on the incident, there's a lesson to be learned about the potential consequences of giving away our private information and how easily it can end up in the wrong hands if we're not careful. Judging by how many people downloaded FaceApp without a second thought, this likely won't be the last time we go down this road.

For all the hand-wringing they've caused, FaceApp's user agreements are really not that egregious. The app only became controversial because the developer is based in Russia. If that same language was for an app from a Silicon Valley company, nobody would bat an eye.

From a data privacy perspective, we give far more personal information to various forms of technology that we use every day, such as social media platforms or Google Android devices. The Android OS itself has gained popularity because of its lower price point, but in reality it's essentially a data collection platform that monetizes information about its users.

In the United States, we're really in the Wild West when it comes to data privacy rules. While the end-user agreements for software need to adhere to any applicable federal or state laws, U.S. data privacy laws aren't nearly as strict as those in the European Union, which implemented its wide-ranging General Data

continued next page

Protection Regulation in 2018. Until our laws in the U.S. catch up, developers have a fair amount of latitude in what they include in end-user agreements, what personal data they collect, and how they use it.

The secret behind free apps

While we've grown accustomed to downloading all kinds of free or low-cost apps, we haven't truly accepted the reality that there's still no such thing as a free lunch. Those "free" apps still have a price — and that price is the app's creator's use of your personal data. It can cost a company millions of dollars to develop a single "free" app, but they recoup that (and more, of course) by monetizing your data, which they collect as you use those apps.

Most of that monetization comes via targeted advertising, but companies also sell certain private data to third parties as well. It all depends on the terms and conditions you agree to, and the permissions you provide, when you install a new app.

In recent years, there's been a slow creep where we give more and more sources more and more of our data. Think of how many times you've scrolled through an end-user agreement without reading it and clicked "I agree." Even as a data security professional, I know I've done it.

We don't think of our personal information and activities as having a monetary value, but they do. We should be thinking of handing over our personal information in the same way we think about forking over cash. Our personal information has real value, just like cash, and until we truly recognize that, we will continue to simply click that value away.

The best thing you can do is pay more attention when installing a new app on any device. Of course, if we say no to the terms of service, we usually can't install a piece of software or use it to its fullest extent. But that doesn't mean we should automatically say yes when an app asks for access to specific resources on our device. When you make any purchase, you're making a decision as to whether the goods you're purchasing are worth the

continued next page

cash required; the consideration over giving others access to your personal information should be taken just as seriously.

Gaming is a great example. Game apps usually ask for access to your local file system, which speeds up game performance by allowing you to save your place in a game or download components that would stream otherwise. Without granting that permission, you can often still play the game, but it might not run as fast or give you all the options you might otherwise have. So, you have to decide whether what you gain is worth what you're giving away.

Think critically before installing

When installing a new app (or any software), think critically about the data and functions to which it's requesting access and make as intelligent a decision as you can based on what you know. Installation processes have become much more transparent in disclosing the types of data to which the app is requesting access. In most installation processes, while there's still a long end-user license agreement, it now will inform you specifically what personal data and which device functions the app deems necessary, and then it'll ask you to give permission for that access.

Pay close attention; if you don't see a reason for an app to need access to the particular information or functions it's requesting, just say no. If a new game asks for permissions to your contacts, for example, it's likely a good thing to say no, as there's little or no reason it would ask for such permissions other than to promote products.

You're better off being more restrictive than blindly saying yes to everything. If you change your mind, you can always uninstall and reinstall the app or change its settings where available. Indeed, that's one of the oldest data security strategies: It's always better to restrict access to data and open it as needed than to try to put the toothpaste back in the tube.
When it comes to data security, it's important to remember that, aside from what we actually know and understand today, we don't really know how our data will be used in the future. Thus, if we don't put reasonable restrictions on

continued next page

access to our data now, we lose the ability to control it once it's out in the wild, and who knows what it might be used for in the future.

Facebook, Google, Apple and other software developers are making their data privacy policies clearer and easier for users to understand and control. But never assume that you're being told everything. The more companies reveal to us exactly how they're using our data, the more likely we are to alter our usage of their apps and services, which directly impacts revenues and profits. So, as much as companies talk about increasing transparency, there will always be an incentive for companies to use your data in ways not clearly disclosed or foreseeable.

Ultimately, as consumers, we're entitled to know what a product or service costs before we make a purchase decision. In the simplest of examples, you don't go into a restaurant and order food without knowing what it's going to cost. We need to look at "free" apps no differently and understand that there is a cost to those apps after all. Sure, many people are still just going to click yes to everything without thinking about it. But at least, with clearer privacy policies and a little individual diligence on our part, we have the option to make better, more informed and more meaningful decisions. And that's a step in the right direction.

Brian Schrader, Esq., is president & CEO of BIA, a leader in reliable, innovative and cost-effective eDiscovery services. With early career experience in information management, computer technology and the law, Brian co-founded BIA in 2002 and has since developed the firm's reputation as an industry pioneer and a trusted partner for corporations and law firms around the world. He can be reached at bschrader@biaprotect.com.