Think Before You App

Apps for games, entertainment, photo and video sharing, business, health and fitness, shopping, digital payments, and medical based apps all saw app usage growth since the pandemic started. As our app usage increases, so does our information sharing. We share our game scores on one social media platform. We share photos and videos on another social media platform . We even share the distance we ran or biked, and how many calories we burned. But we don't share things such as banking information, passwords, and our medical information, or do we' As we increase our app use we need to think about the risks to privacy. Privacy Concerns

Privacy is engaged from the moment a user agrees to the collection of their personal information. However, meaningful consent is difficult to obtain and users are often quick to agree to whatever privacy policy exists without reading it. To complicate things more, privacy expectations can depend on when the user made their account, last logged in, and if they read updated policies before quickly closing pop-ups to use the app.

Furthermore, some apps may store and access more private information than users would like to think. If the security on those apps are breached, unauthorized access to those apps not only exposes users' identities and contact information, but also possible auxiliary information connected to the app's use such as bank accounts, address books, photos and videos, and location data. A breached account can then be stolen, deleted, secretly viewed, or used to post or expose content without the

original user's consent. A privacy attack can also prompt users to click phishing links that inject malicious code into trusted websites, which further augment security concerns and have ripple effects to other private information. These issues are particularly prominent in new apps that have yet to be tested and scrutinized by the public to reveal vulnerabilities in the app's security.

Given the vast amount of identifying and private information that may be stored and used by smartphone apps, it is important that policies clearly define privacy rights and ensure that any policies comply with applicable privacy legislation. Falling short of privacy laws can be costly. Even an app's perceived security concern can have serious implications, such as being banned on government issued smartphones.

Takeaway

Consumers, businesses, and governments need to consider whether sensitive information could be breached through an app. For example, limiting sensitive information to encrypted devices or using separate devices for non-essential apps may be a better way to secure private information and limit privacy concerns.

In a competitive app market, will the new wave of apps compete to be the most secure in their respective field or will the scales of convenience vs. privacy remain uneven'

About Norton Rose Fulbright Canada LLP

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have 3800 lawyers and other legal staff based in more than 50 cities across Europe,

the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

by Daniel Daniele
Norton Rose Fulbright Canada LLP