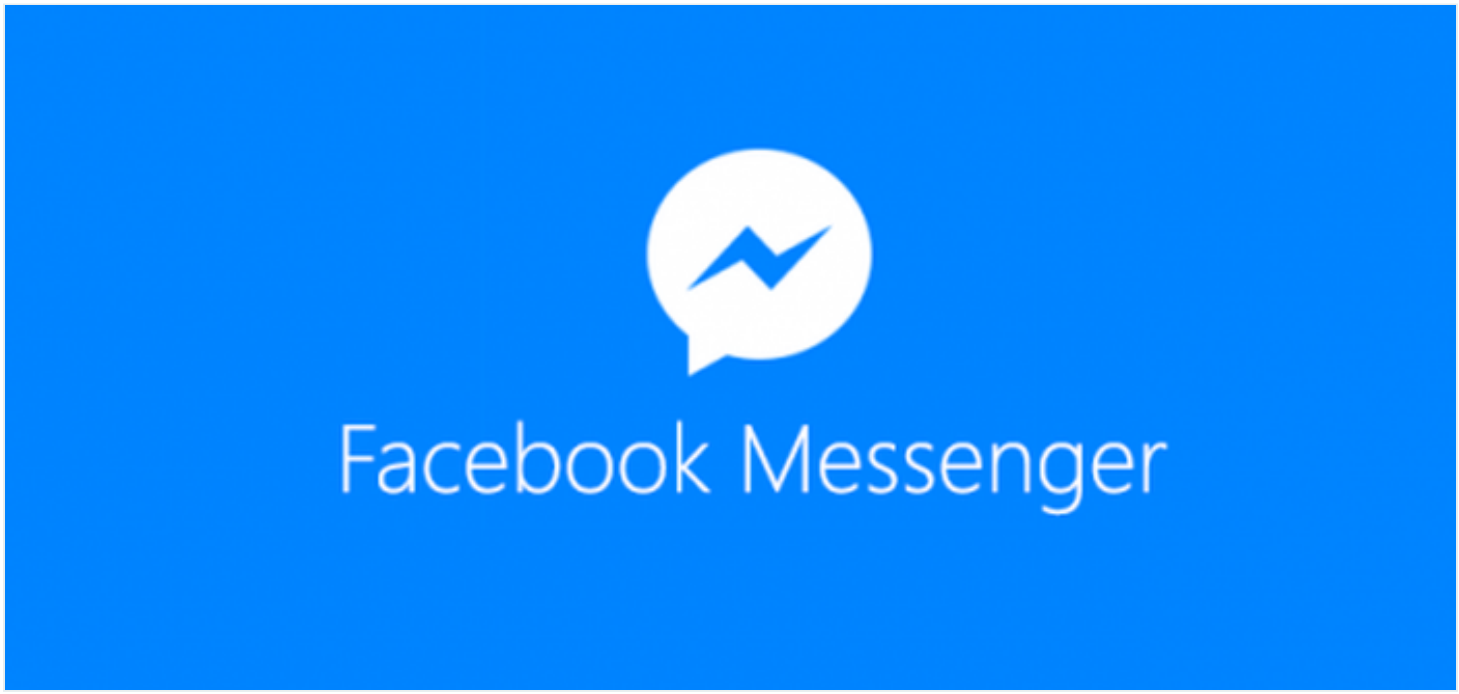
scramble to find revenue beyond the simple sale of software or services. And they have a ready-made opportunity in collecting and selling the personal data of their users ...

Dave McClure • Mar. 07, 2016



When the economy gets tight, markets grow more competitive and some players scramble to find revenue beyond the simple sale of software or services. And they have a ready-made opportunity in collecting and selling the personal data of their users, which can then be sold to marketers, spammers and identity thieves.

It may seem unfair to lump legitimate marketers with scammers and thieves, but the reality is that the collection and use of this data provides a safe and legal cover to the bad guys. They aren't doing anything wrong, just sharing customer data with a few "associates." Any anti-theft systems protecting the data is immediately rendered ineffective.

Thus we have seen the debut of software such as Samsung's My Magazine, powered

permission to access the user's location, calendar, camera, access to unique identifiers for the phone, and then share data with a number of ad networks, including Google's AdMob, iAd, and JumpTap. The app has not been shown to actually collect and forward all of this information, but the fact that it is requested raises red flags.

One flashlight app developer, Goldenshores Technologies (makers of the "Brightest Flashlight" app for Android), did settle a complaint with the FTC in 2014 over the collection of location data and unique device identifiers from users' devices and sharing that data with advertisers.

And now Facebook, never considered a strong champion of privacy, is forcing its users to install a new chat and messenger application or face continuous nag screens. Only in the fine print will you find the fact that use of the app gives almost total control of the device on which it is installed — access to all pictures, videos, the microphone, and the camera. Again, there is no evidence that this information is being sold or given to third parties. But it follows on the heels of another effort by Facebook to request your cell phone number – allegedly to enhance the security of your personal data. There is only a cursory explanation as to why this might be necessary.

The installation process for applications does list the features to which you are giving access. Unfortunately, most users do not read this warning during installation or do not understand what it means. The warning notes what data will be collected by each application, including:

- A log of all In-app Purchases
- Sensitive log data system internal state
- Web bookmarks and history
- A list of running apps

- Your identity

data, but the mere fact that the capability exists invites someone to try to misuse it. Imagine how merger negotiations might be compromised if opposing parties can use your cell phone – even if turned off – to identify who is at the meeting and listen in. Or have the ability to access the tax files on your office computer.

The *FTC Standards for Safeguarding Customer Information Rule (16 CFR Part 314)* requires financial institutions, as defined, which includes professional tax preparers, data processors, affiliates and service providers to ensure the security and confidentiality of customer records and information. That can't be done if you have no control over the data that is accessed by "benign" applications.

Exactly how much liability a CPA firm might incur has not yet been tested in court, but that day is surely coming. The opportunity exists for your client data to be compromised, a profit motive already established, and accounting data has become one of the hottest commodities in the marketing and hacker realms.

A well-managed firm will still take notice, and take corrective actions.

Firm Management • Security