

Big-name travel apps may secretly record your iPhone screen, including credit card info



A number of popular airline, hotel, and retail apps engage in the practice of recording your iPhone screen without your knowledge or consent, according to an investigation from *TechCrunch*. The practice, known as session replaying, typically involves hiring a third-party firm, in this case the analytics firm Glassbox, to embed the technology into a mobile app.

From there, Glassbox's software records every action you take within the app, as well as taking screenshots along the way. Even worse is that, for apps like Air Canada's and other travel sites, this includes the fields where users input sensitive information like passport numbers, credit card numbers, and other financial and personal information.

According to *TechCrunch*, none of the most widely used travel

or retail apps that it could find that employed Glassbox's technology disclose this in a privacy policy or similar public-facing document. Additionally, it doesn't seem like any of these apps have received consent from the user in any way. Among the apps mentioned in the investigation include Air Canada, Abercrombie & Fitch and its Hollister subsidiary, Expedia, Hotels.com, and Singapore Airlines, among others. *TechCrunch* based its report on information unearthed first by the App Analyst, a mobile security blog.

Air Canada's app didn't properly mask session replays that included sensitive info

While this would appear to be a common practice in the mobile app industry, what makes it especially worrisome is that the App Analyst discovered that Air Canada in particular was not properly masking its session replay files when they were sent from a mobile device to the company's servers, meaning they're vulnerable to a man-in-the-middle attack or other similar interception technique. Back in August of last year, AirCanada reported that its mobile app suffered a data breach, exposing 20,000 users' profile data that may included passport numbers and other sensitive identifying info.

As *TechCrunch* notes, none of the apps that engage in screen recording for analytics purposes disclose this to users. That suggests there could be a number of other iOS apps, as well as Android versions too, that use session replays, and in such a way that leaves the information recorded through the app vulnerable to a hacker or other malicious third party.

And while it may not be all that surprising that numerous companies out there collect this type of data, it does highlight how these large corporations exploit the lack of understanding most mobile app users have around privacy, data collection, and app analytics. When the *Wall Street Journal* revealed that Google lets third-party email app developers read your Gmail messages, it caused an uproar from users and members of Congress who were largely unaware of the practice,

even though you might reasonably call it industry standard.

In this case, it may be less about the intrusion into how you use, say, the Expedia app in your free time and more about the potential risk you face when Expedia insecurely sends a video displaying your credit card number back to its own servers.

<https://www.theverge.com/2019/2/6/18214578/apple-iphone-ios-session-replay-apps-recording-screen-hotel-travel>