This article was originally published in eGR Mobile Intelligence

TAKING A PEEK AT YOU

STRATEGY
PRIVACY

JAMES LONGSTER, SENIOR ASSOCIATE AT LAW FIRM TRAVERS SMITH, DISCUSSES THE PRIVACY ISSUES REGARDING THE POKÉMON GO APP AND BEST PRACTICE FOR APP DEVELOPERS

Much has been said in the press recently regarding the overwhelming success of Niantic's Pokémon Go app (at the time of writing it is still the number one app on Apple's US App Store), but a great deal of press coverage has also been given to the problems it has caused.

These problems have ranged from the mass congregation of people at Pokémon "gyms" to the unfortunate appearance of a Pikachu at Arlington Cemetery. But from a legal perspective, one of the main problems has been the app's almost complete disregard for its users' privacy.

As has now been well documented, the Pokémon Go app had complete and unfettered access to the Google accounts of anyone who had registered with the app using their Google account on an Apple device.

This granting of "full access" enables the app to read and send emails from the relevant Gmail account, view and edit Google Drive documents, access photos and much more.

Did Niantic actually mean to do this though? Either way, it doesn't look good for Niantic from a PR perspective – they were either purposefully ensuring they had full access (in which case, we have to query why they wanted it), or they simply failed to take sufficient care in relation to privacy issues. From a legal perspective, neither answer is good enough.

The approach taken by Niantic flies directly in the face of the European data privacy concept of Privacy by Design (i.e. when you are creating a system, developing an app etc. that will process personal data, you should have the protection of privacy as one of the central planks of your thought process).

While Privacy by Design has been discussed as a concept in privacy circles for a number of years (and is currently best practice), it will formally become part of European legislation when the General Data Protection Regulation (GDPR) comes into force in May 2018.

This may seem to many as though it is a solely European problem, but the territorial scope of European privacy legislation will significantly increase under the GDPR to include the processing of personal data relating to someone in the European Union (regardless of where the data controller is). An app developer in, for example, the US will need to consider European data protection legislation if the app is going to be aimed at (or accessible by) people in Europe.

So what steps should an app developer take in an effort to ensure compliance with EU data protection legislation? The main considerations are:

1. Ask yourself whether your app will be collecting any personal data (i.e. information that identifies/relates to an individual – including geo-data and IP addresses) – the answer to this will usually be "yes" – and what that personal data is.
2. Ask yourself what you want to do with the personal data and whether you need it. If you don't need the personal data, you generally shouldn't be collecting it in the first place (i.e. you want to avoid what Niantic did).
3. How are you obtaining consent to what you want to do with the personal data? "Express" consent will be particularly important if you want to commercialise the personal data (e.g. marketing to the user or selling it to a third party). It's also worth remembering that obtaining consent will be more difficult under the GDPR as it will be more difficult to rely on "implied" consent.
4. Ask yourself how you are keeping the personal data secure; do you comply with best practice information security measures?
5. Keep your approach to data protection under review with regular security tests etc.

A failure to consider privacy issues can lead to negative publicity and potential monetary penalties; these penalties will significantly increase under the GDPR as European regulators will have the power to fine data owners up to the greater of €20,000,000 and 4% of global turnover. There is no one-size-fits-all approach to data protection, but it should be something that app developers have in their mind from the outset. ⬣