Angry Birds will have angry users until privacy rules are clear

January 30 2014, by Arosha K Bandara

Would you trust this guy with your personal data? Credit: tomazstolfa

It was reported this week that the NSA and British intelligence agency GCHQ have been gathering information from popular apps including David Cameron's favourite game, Angry Birds.

According to the Guardian, the spy agencies have been working since 2007 to develop the means to take advantage of "leaky" smartphone apps

by sucking up user details when they are transmitted across the internet. This could include usernames and location as well as make and model of the phone being used. It is even being suggested that highly sensitive information such as sexual orientation can be gathered.

As the app market grows ever bigger and more small companies get in on the act, these latest revelations raise important questions about who is responsible for user privacy and protection when an app is developed.

What they know about you

Any company that is in the business of selling a mass-market product will be interested in gathering as much information as possible about the consumers in the marketplace. In most cases, gathering this information would involve getting some subset of the consumers to participate in a survey and use statistical analyses to extrapolate the results to the wider population.

But these techniques are expensive and difficult to implement because they require the active participation of the consumers. They need to be convinced to give up their time to fill in surveys or even take part in a face-to-face interview. That all costs time and money for the business.

This has all changed in the world of smartphone applications. App producers have the unique capability to passively gather a lot of information about their consumers because their products are necessarily used on an internet connected device. These devices have increasingly sophisticated sensors and, as a result, companies can very easily find out when you use their application, for how long and even what type of device you are using.

With a little additional effort they can also access information such as your contact list, call history, location, the list of other applications you

have installed on your phone and which of these are running at the same time as theirs. The developers find this information useful because it allows them to figure out how to make their application better, such as by working out what makes it crash.

There are also a number of software services, such as Flurry, that provide data analysis services using this data to infer additional information such as gender, age and area of residence by combining the data gathered across multiple application providers.

The fact that all this information can be collected and transmitted across the internet means that it is vulnerable to intercept by other parties. And that includes national intelligence agencies.

You read the terms and conditions, right?

Different approaches to help mobile application developers think more systematically about the security and privacy implications of their software as they work have already been suggested. For example, the Canadian Information Commissioners office developed an approach called Privacy by Design and the mobile operators' interest group the GSMA developed a set of design guidelines for mobile app developers that are based on a number of privacy scenarios.

These are useful to many but they do still require developers to think about privacy at every step of the way and, crucially, to be able to explain the privacy issues relating to their product in a way that is understandable to users.

This means it is up to the end user to check the terms of the licence agreement and understand the security and implications of the behaviour of the app. Of course this isn't a very practical approach since most end users don't have the expertise, or inclination to do these checks. App

developers generally get your permission for gathering personal data as part of the end-user license agreement you accepted when you downloaded the app, but probably didn't read.

Angry users

When a high-profile game such as Angry Birds turns out to be yet another vehicle for spying, users naturally become more aware of threats to their privacy. But in this case and many others, ignorance may prevent them from taking measures to protect themselves. Even though they know there is a problem, they don't have the knowledge and means to do anything about it. How do they identify which apps have these vulnerabilities against those that do not?

This lack of ability to control our own privacy is an issue that must be addressed and different options have been mooted.

Bringing in Privacy Nutrition Labels that help users get a quick understanding of what data an application gathers is one. Another is a system through which developers build an argument as to how their application meets the privacy needs of end users, which app marketplace platforms could use as the basis for certification.

The terms and conditions of apps are often fluid and need to be amended over time. They are, by their very nature, difficult to understand and unlikely to be read. This means that until we make it easier for users to enter into contracts with app developers with their eyes open, breaches like we've seen with Angry Birds will continue to happen.

It seems unlikely that people will stop downloading blockbuster games on their phones over fears they will be spied on. But of course one group of people may well do just that – those the NSA and GCHQ want to target the most. They may become hyperaware of the dangers of taking a

break with Angry Birds and stop using these applications altogether. That still doesn't mean you can skip the terms and conditions reading, though.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation