Privacy Compliance in Apps—an Important Agenda Item in 2015

This article was originally published on Telecoms.com on February 3, 2015.

by Rafi Azim-Khan and Steven P. Farmer

Rafi Azim-Khan
Global Sourcing
+44.20.7847.9519
rafi@pillsburylaw.com

Rafi Azim-Khan is head of Pillsbury's Data Privacy practice in Europe and leads the firmwide Marketing Law Team. He is a partner in the Intellectual Property and Information Technology practices.

Steven P. Farmer
Global Sourcing
+44.20.7847.9526
steven.farmer@pillsburylaw.com

Steven Farmer is a senior associate in Pillsbury's London office and is a member of the firm's Global Sourcing practice and Intellectual Property/IT, Data Privacy and Marketing Law teams.

A 2014 survey of over 1,200 of the top mobile apps in 19 countries by the Global Privacy Enforcement Network ("GPEN") found that 85% of the apps reviewed were non-compliant, failing to provide even the most basic privacy information to users.

In addition, 43% failed in their obligation to tailor privacy notices to smaller screens and almost 30% unlawfully requested excessive personal data from users.

The GPEN's survey was subsequently followed up by an "EU Cookie Sweep Day", conducted by a number of European regulators last autumn, to assess websites' and apps' compliance with EU rules requiring them to obtain consent before installing or reading cookies.

All this suggests that the European enforcers are circling and smell blood, with results of the cookie sweep expected over the coming months and enforcement action expected to follow thereafter.

The EU Cookie Sweep Day and what the law says

The various European regulators assessed the levels of compliance on "hit lists" of the most visited websites/apps targeting customers, per territory, whether they operated inside or outside the EU.

The sweep focused on the number and types of cookies in use, the quality and visibility of the cookie information communicated to users, the way in which consent was obtained and the consequences for a user refusing cookies.

By way of background, under EU law (implemented in the UK by virtue of the Privacy and Electronic Communications (Amendment) Regulations 2011, which came into force on 26 May 2011), if cookies are used by a website/app, certain information must be given to a visitor and the visitor must give his or her consent to the placing of cookies, unless a limited exception applies.

The Regulations mean that a website/app operator must not store information or gain access to information stored in a web-enabled device unless the user is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information and has given his or her consent.

The only cookies which do not require consent (which is defined in the Data Protection Act 1998 as "any freely given, specific and informed indication of wishes") are those that are "strictly necessary" to fulfill the user's request for services e.g. those that remember the contents of a user's shopping basket as the user clicks through a site's pages.

Should app developers care about these findings and developments?

In short, yes, especially given that the UK privacy regulator, the Information Commissioner's Office ("ICO"), has recently conducted additional research that demonstrates that around half of app users have decided against downloading an app due to privacy concerns at some point in time.

Risk for developers does not stop there either.

As has been well reported elsewhere, privacy regulators in Europe now have the power to fine developers "on the spot" who breach relevant laws. For example, in the UK, the ICO has the power to issue fines up to £500K.

Some regulators, including the ICO, have further announced that "mobile" has now been moved to the top of the enforcement agenda. In other words, the regulators do have a stick and they appear willing to use it.

When brand damage associated with any enforcement action (such actions are published) and potential civil action is thrown into the mix, this could well compound problems, or even sound the death knell, for any developer who chooses to ignore privacy compliance.

I'm an app developer—what should I do?

The ICO has published guidance for app developers to help them understand their legal obligations when collecting personal data and to ensure users' privacy. By adhering to this guidance, developers will be much less likely to fall foul of EU/UK privacy laws and find themselves on the end of an enforcement action.

The guidance covers key issues such as how to communicate privacy related information to users, how to obtain meaningful consent from users (all in the context of a small screen), as well as how developers should keep information within an app secure.

Top tips for privacy compliance during app development include: (i) using "in-time" notifications when more intrusive data is being collected, e.g., GPS location data; (ii) using links to separate sections of a privacy policy and to keep things short and snappy (given the size of screens involved); and (iii) avoiding being legalistic in language used in privacy notices.

Where an app uses cookies it is also important to first audit how cookies are used and understand how intrusive they are, explaining in the policy how and why they are used.

Whilst the ICO suggests various methods that can be used for obtaining consent for cookies, the key is for businesses to find a solution which works best for them.

Comment—further developments on the way

This app sweep by GPEN and the "EU Cookie Sweep Day" are some of the latest initiatives which suggests regulators are taking compliance issues in this area much more seriously and that a greater use of enforcement action is on the horizon.

The time is ripe, therefore, for developers to audit their data collection and data use activities and to review the policies they have in place to assess their exposure to regulatory enforcement. Transparency and clarity are key. Adhering to such principles should not only help keep the regulators at bay, but also have a significant effect on a developer's bottom line.

This is particularly poignant when it is borne in mind that a new EU Regulation for data protection is on the horizon. This new Regulation is expected to grant regulators with additional weapons to use against those who break the law. Given possible fines of up to 5% of a company's global turnover are being pushed for by the European Commission where serious breaches of privacy legislation occur, those in the app lifecycle are well advised to push data protection compliance up the board agenda and to take such issues seriously if they are not already.