Question for written answer E-011538/2015
to the Commission
Rule 130
Ivan Jakovčić (ALDE)

Subject: Privacy issues on mobile devices

App developers who are unaware of data protection requirements may create significant risks to the private lives and reputations of users of smart devices. The key data protection risks to end-users are a lack of transparency and awareness of the types of data processing an app may undertake, combined with a lack of meaningful consent by themselves before that processing takes place. Poor security measures further contribute to the data protection risks found within the current app environment.

Many types of data available on a smart mobile device are personal data. The relevant legal framework is the Data Protection Directive, in combination with the protection of mobile devices as part of the private sphere of users contained in the ePrivacy Directive.

However, although the users' consent is required, some permission requests, such as the possibility to activate the camera or the possibility to read data stored in the card, are too invasive and many people can actually take control of the device.

How can the EU prevent those violations of individuals' privacy that are really threatening to the lives of millions of EU citizens?