Dr Joasia Luzak

**A house of bricks? On the 3rd version of e-Privacy Directive – from the post-Brexit UK perspective**

This paper poses a question whether it is possible to draft the third version of the e-Privacy Directive (the “Directive”) in such a way as to provide it with solid fundaments, capable of protecting internet users’ privacy and their trust in online transactions, regardless of new challenges posed by evolving technology (‘the big bad wolf’). Moreover, it considers the feasibility of adoption of these new rules by the post-Brexit UK and the likely consequences of lack thereof.

The paper first discusses the public consultation of summer 2016 on the revision of the Directive, which clearly showed conflicting interests of consumers, industry and public authorities. These conflicting interests will be hard to reconcile by the European institutions, and may, again, lower the level of privacy protection in the final version of the Directive. This notwithstanding the fact that the European Data Protection Supervisor called in its opinion 5/2016 upon EU institutions to reinforce privacy protection, not only by adjusting the scope of the Directive to the General Data Protection Regulation. The public consultation revealed three main issues that the revision should tackle, which this paper explores.

First, with regard to the scope, the Directive is currently not meant to protect privacy in such technologies as, e.g.: cloud computing; over-the-top services; facial recognition; which have all developed after the adoption of its last version. Second, current rules are vague, which means that there is no clarity as to, e.g.: whether metadata (traffic and location data) is covered by confidentiality rules; what way of obtaining informed consent for gathering users’ data is compliant. Third, rates of compliance and enforcement are low, and in different Member States different authorities have purview over this area.

After examining the above-mentioned issues and proposing a revision’s scope that would enable the EU legislator to build ‘a house of bricks’ around internet users’ data, protecting their privacy and increasing their trust in the online environment, this paper turns towards the specific case of the UK. Brexit might protect the UK from claims by EU institutions of improper adoption of the Directive. For example, the Information Commissioner's Office’s communication of 2012 stated that 'wherever possible' placing of cookies should be delayed till consent is obtained. Such a backdoor for obtaining informed consent was not envisaged by the Directive’s drafters. This ‘flexible’ implementation does not surprise, considering privacy protection was never recognised as a fundamental right in the UK, prior to joining the EU. Unfortunately, the UK will likely not be obliged to adopt the Directive’s changed rules, as the implementation deadline might fall after Brexit. However, it needs to be considered that the EU might not allow British companies to trade with EU ones, if the UK cannot guarantee the safety of exchanged data and endangers trust in online transactions. This paper indicates, therefore, practical reasons why the UK should follow the EU’s lead in the area of privacy protection.