Executive Summary

User numbers on social networks are increasing steadily. Users continue to share a wide variety of personal and public information on the Internet and are becoming more educated and aware of data protection. This is resulting in an increased desire for better Internet privacy. Social networks, on the other hand, are largely driven by marketing revenue and therefore have a need for an ever-increasing amount of user information in order to generate targeted advertisements. It is increasingly apparent that the interests of users and social networks are conflicting.

The purpose of this report is the review of the user policies of four of the top social networks, as well as of relevant pieces of legislation, in order to determine their adequacy in protecting user privacy. Reviewed were the policies of Facebook, Twitter, Google+ and LinkedIn as well as the U.K. Data Protection Act 1998, the Irish Data Protection Act 1988/2003, the Directive 95/46/EC and the newly adopted General Data Protection Regulation 2016/679 and EU-U.S. Privacy Shield.

As a result of the policy reviews several common areas of concern were found. These are content that is ‘public’ by default, massive data collection, data sharing practices, data retention practices and data transfer insecurities. Users have no control over the massive data collection practices of social networks. Legislation in support of limiting data collection from the outset would be required but, for commercial reasons, this is not likely to occur. The problems with social networks’ data sharing practices stem from their own definition of ‘personal data’. Too much information is deemed ‘public’ and thus freely shared. Anonymisation of data is used as a crutch to allow user data storage even after the user requests account deletion. Some social networks state that they may never delete user information from their backup servers. These are areas where legislation could support the users’ desire for more privacy rights. However, the effectiveness of the relevant pieces of legislation that were reviewed may only be limited. Generally speaking, relevant legislation favours free flow of information for commercial purposes over increased user privacy. The best effort to improve user privacy was seen in the General Data Protection Regulation (EU) 2016/679 (GDPR). The GDPR will vastly improve the quality of communication between social networks and users. Social networks will be obligated to disclose more concise, easy to understand information and to put a maximum limit on how long data may be stored. However, the GDPR is still seen to favour commercial aspects over user privacy and thus is likely to only increase user privacy by a small margin.
The battle between providing an increased level of user privacy and the free flow of information for commercial purposes will continue. Only collaborative pressure from both governments and users may swing the scale in favour of user privacy over annual profits. More realistically, users who choose to use social networks and are concerned with their privacy must educate themselves by carefully reading the policies of such sites and must realise that any information shared will be available to multiple entities. Unless social networks are introduced on a paid-for membership basis, a higher level of user privacy will not be achievable.

Issues raised in this paper have been updated as much as possible up to July 31, 2016. While writing this paper the United Kingdom (U.K.) has also made the decision to leave the EU (European Union). In the near future this will affect the relevance of EU specific pieces of legislation depending on whether the United Kingdom will adopt such practices or choose to use only U.K. specific data protection requirements. Because of the on-going changes occurring presently, some information or relevancy of information presented in this paper may have changed by the time it is submitted.