Abstract

As the number of Facebook users across the globe reaches over a billion, more people continue to make even greater use of this social network to support their daily activities and relationships. As a result a large amount of personal information is being generated, all of which provides extensive insight about Facebook users. This information is frequently exposed to other individuals in unexpected ways and often with severe consequences such as shame, embarrassment, job loss, and sometimes even arrest. Additionally, this large collection of users' personal data is owned and stored by Facebook, which now exploits it for money through advertising, in continually changing and often bewildering ways.

This research paper aims to address the complex and often controversial debate around privacy invasions, specifically with regard to Facebook and the alternative social network site Diaspora*. It develops a rigorous conception of privacy relevant to online social networks, primarily using Helen Nissenbaum's framework of contextual integrity. This conception is made up of two dimensions: social privacy and institutional privacy. Social privacy generally covers *peer-to-peer* violations, while institutional privacy covers the relationship between Facebook and its users, specifically its practices regarding user data. These conceptions of privacy are used in conjunction with an analysis of Facebook's history and current privacy policy and features to determine the nature of privacy violations on Facebook, and the extent to which Facebook is accountable. This analysis occurs in the time frame since Facebook's inception in 2004 until June 2012, a month after its Initial Public Offering. As a comparative case study, the conception of social network privacy is used to assess the "Anti-Facebook" alternative social network Diaspora* to determine whether it successfully offers a better solution to social network privacy than Facebook does.

This paper concludes that violations of social privacy occur on Facebook primarily due to the collapsing and convergence of many different contexts. Institutional privacy is

violated by Facebook's continually changing, dense and bewildering data practices, which is exacerbated by the centralised nature of its user data store. Facebook is accountable for these violations principally because its default settings continually push towards increased information disclosure. This paper also concludes that this push is intentional, in light of Zuckerberg's fanaticism about making the world more transparent, and because of the commercial value of Facebook's huge personal data store.

This paper also concludes that Diaspora* offers some improved solutions to maintain online privacy, primarily because of the control of data it provides to its users and because of its potential to promote a heterogeneous landscape of social networks that do not need to commercially exploit user data. However, Diaspora* introduces some further risks to institutional privacy, and it is asserted in this paper that some social privacy issues are intrinsic to online social networks, and therefore difficult to avoid.