You have zero privacy. Get over it.¹

Unlike Vegas, what happens in Facebook doesn’t stay in Facebook.²

Sharing is the euphemism for selling and commodifying data. Facebook commodifies and trades user data and user behaviour data. Facebook does not make the world a better place; it makes the world a more commercialised place, a big shopping mall without an exit.³

Introduction

This chapter critically reflects on the way in which hugely popular social network media platforms around the globe including Facebook, Twitter, Weibo, QQ, Cyworld, Mixi, VK, targeted advertising and locative media apps have become ground zero for new media privacy. The near ubiquitous use of mobile devices has spread social media networking as an activity that everyone can be involved in, from virtually any location, assuming the user has an Internet connection.

With the share buttons of social networks now embedded in the online sites of traditional and new online media brands, the potential threats to personal privacy have been greatly extended. While demographics may have initially played a role in these developments, with greater take-up in all ages and groups they are becoming
less significant. Social game apps have become a site of intense regulatory action (e.g. by the FTC in the US), as the privacy rights of users, particularly children, have been found to have been in breach of controversial Children’s Online Privacy Protection Act and other ‘Do not track’ laws. Equally, where digital content ‘cloud’ management systems run in parallel and interact with social networking platforms, these are creating their own specific sets of concerns as they get to ‘know’ their users, their likes, dislikes and detailed consumption patterns. Popular music serving software brands like Pandora and Spotify are examples of how audiences are enthusiastically responding to ‘intelligence’ in their media content delivery.

With these interactions occurring while people are on the move, devices including smartphones and iPads disclose geographically specific personal information to networks and to third parties. The clear trend is for commercialised media storage and distribution systems to amass and then rely on a more targeted personal consumer data for further business purposes.

Third party businesses and applications often appropriate personal information and use it in ways that people are unaware of, and therefore, without their consent.

Innovation in retail data analytics, including software tracking consumer’s real-time shopping, is just one development that is chipping away at people’s expectation of privacy. A company that trades as ‘Skyfii’ in Australia is a case in point. This company supplies and manages guest wifi in major shopping mall centres, and then provides a data analytics service to assist in targeting specific customers. Consumers in shopping malls first register to use the free wifi service, and then Skyfii tracks shoppers’ behaviour and ‘internet and social media use in real time, including the time they spend in stores and the websites they browse while shopping’. Skyfii uses this data to then send messages to shoppers on behalf of retailers, and it also provides feedback to retailers with suggestions about how to encourage customers to spend more. They are not the first company to exploit personal data in a high street or shopping mall context: the Renew advertising firm in the UK was involved in a similar practice in 2013 involving high tech rubbish bins. The CEO proudly boasted to a reporter that his firm would ‘cookie the street’: as shoppers stroll by, wifi sensors track iPhones to track people walking through London’s financial district. The idea in this case is that targeted