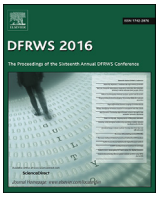
Digital Investigation xxx (2017) 1–11

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin



A survey of current social network and online communication provision policies to support law enforcement identify offenders

Graeme Horsman

Faculty of Computer Science, The David Goldman Informatics Centre, St Peter's Way, Sunderland, SR6 0DD, United Kingdom

ARTICLE INFO

Article history:
Received 25 October 2016
Received in revised form
16 February 2017
Accepted 27 March 2017
Available online xxx

Keywords:
Social media networks
Crime
Regulation
Internet
Cyber crime
Harassment

ABSTRACT

Online forms of harassment, stalking and bullying on social network and communication platforms are now arguably wide-spread and subject to regular media coverage. As these provision continue to attract millions of users, generating significant volumes of traffic, regulating abuse and effectively reprimanding those who are involved in it, is a difficult and sometimes impossible task. This article collates information acquired from 22 popular social network and communication platforms in order to identify current regulatory gaps. Terms of service and privacy policies are reviewed to assess existing practices of data retention to evaluate the feasibility of law enforcement officials tracking those whose actions breach the law. For each provision, account sign-up processes are evaluated and policies for retaining Internet Protocol logs and user account information are assessed along with the availability of account preservation orders. Finally, recommendations are offered for improving current approaches to regulating social network crime and online offender tracking.

Introduction

Online platforms have now revolutionised modern day communication. However, in light of recent global events, social media has now become a platform for those to voice both positive and negative sentiment, requiring greater regulation by both the social networking sites themselves and the police (Awan, 2016). With a reported 2.3 billion social network users worldwide (Statista, 2016), the regulation of user behaviour on these platforms is a difficult task. In 2015, Vodafone and YouGov surveyed around 5000 teenagers across 11 countries, where 41% of respondents admitted to feeling depressed or helpless from acts of cyberbullying and a further 18% feeling suicidal (Vodafone, 2015). In addition, a quarter of those surveyed had actively closed their social media accounts due to acts of cyberbullying (Vodafone, 2015). Similarly, the Association of School and College Leaders (2016) reported that 41% of the school leaders surveyed reported an increase in acts of students being cyberbullied. In 2016, anti-bullying charity Ditch the Label (2016) surveyed 8850 persons aged 12–20, with 6 out of 10 of those reported to have been bullied, indicating that they had experienced this online. Despite the many benefits offered by online communication and social networks, a darker side is also apparent.

Social networks and online forms of communication are frequently identified as problems in the battle against online harassment and abuse. In 2014, 'a total of 38 out of 45 police forces saw a rise in the number of crime reports that involved Facebook' (Birchley, 2015) with 'the Metropolitan Police, receiving 1207 crime reports which mentioned Facebook, up from 935 in 2013 and 997 in 2012' (Evans, 2015). Further Evans (2015) reports that over '16,000 alleged crimes involving Facebook and Twitter were reported' across all United Kingdom (UK) police forces for the period of 2014/15. The Twitter platform is regularly subject to scrutiny due to the volume of trolling (an act of posting 'inflammatory or inappropriate messages or comments online for the purpose of upsetting other users and provoking a response' (Dictionary.com, 2016)) which occurs (BBC News, 2016a) and the service has been criticised for failing to be proactive in regulating and removing offending content, such as that posted by the extremist cleric Anjem Choudary (BBC News, 2016b). Other examples of social network abuse include the 2011 England riots where such provision were used to organise mass congregations and crime, with Williams et al. (2013) suggesting that at the time, police were ill-equipped to deal with analysing this content. Yet it remains questionable as to whether some 5 years later, law enforcement are in a better position to

E-mail address: graeme.horsman@sunderland.ac.uk.

http://dx.doi.org/10.1016/j.diin.2017.03.001
1742-2876/

tackle these issues.

Reports of sexist and misogynistic comments targeting those on YouTube and Twitch have also received media coverage (BBC News, 2016c), yet such incidents form merely a small part of a far greater issue. Frequently high-profile personalities are targeted, where recent examples include Stephen Fry, Jennifer Lawrence, Matt Lucas and Sinead O'Connor, prompting their exit from such platforms (Cohen, 2014). In addition, attacks upon Sara Payne, the mother of murdered school girl Sarah Payne, and Zelda Williams, the daughter of the now deceased Robin Williams show an altogether more sinister side of the harassment which can be suffered online (Cohen, 2014). These instances form only a small subset of the overall volume of abuse which is experienced by everyday individuals. Acts of online abuse can now be considered relatively common and form part of a greater issue and debate surrounding the need for greater regulation of social networks, a point alluded to in the House of Commons Home Affairs Committee (2016) report into Radicalisation.

> Social media companies are consciously failing to combat the use of their sites to promote terrorism and killings. Networks like Facebook, Twitter and YouTube are the vehicle of choice in spreading propaganda and they have become the recruiting platforms for terrorism. They must accept that the hundreds of millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of responsibility and ownership for the impact that extremist material on their sites is having (House of Commons Home Affairs Committee, 2016, p.34).

Hate crime is also becoming an increasing issue for social network platforms. In the wake of the UK's vote to leave the European Union (commonly referred to as 'Brexit'), MP Andy Burnham highlighted a subsequent fivefold increase 'in race hate comments on social media channels' (HC Deb, 2016). This is backed by GLA Conservatives's (2015) survey which reported 68% of the 308 individuals reviewed had encountered hate crime online. The Mayor's Office for Policing And Crime (MOPAC) (2016) states that currently social media is providing offenders with a 'veil of anonymity' which is prohibiting effective regulation of their conduct, and have recently acquired funding from the Home Office Police Innovation Fund (PIF) to develop an online hate crime hub (MOPAC, 2016).

In any of the aforementioned acts, where forms on online content overstep the mark and fall foul of domestic or international legislation, the identification on an offender is key to the effective regulation of illegal behaviour. Studies have shown online environments can 'lower behavioural inhibitions', encouraging disclosures and derogatory actions (Suler, 2004; Lapidot-Lefler and Barak, 2012), yet where an account holder cannot be identified there is a lack of accountability for their conduct. This provides an issue for law enforcement when trying to regulate and apprehend social network offenders, potentially leaving any victims vulnerable for sustained online abuse. This article examines the terms of service, privacy policies and functionality of 22 social network and communication provision in an effort to establish the current feasibility of tracking offenders who post content on these platforms in breach of both policy and law. Account sign-up processes are evaluated along with policies for the retention of data which could be used to identify those in breach. Finally, conclusions and recommendations are drawn.

Regulatory problems

Guidelines supporting those subject to cyberbullying and online harassment on social networks exist on various organisation portals designed to support those subject to these acts. Childline (2016) identify Facebook, Twitter, Instagram, Instant messaging (IM), Snapchat, ASKfm and Tumblr, and provide guidance for those subject to abuse on these platforms and how to block and report it. The charity 'Family Lives' (2016) provides guidance on dealing with cyberbullying on Facebook, Twitter, Youtube, Whatsapp, Snapchat and Instagram. Other charities offering similar advice and resources include The CyberSmile Foundation (2016) and the NSPCC (2016). Policing social media content is notoriously difficult and arguably, we are yet to see effective forms of regulation in force across many platforms. The Select Committee on Communications's Report (2014) indicated that this is due to the fact that 'there is no consistent attitude taken by website operators: some require the use of real names (Facebook, although they do not actively confirm users' identities); some allow anonymity but challenge impersonation (Twitter) and others allow absolute anonymity'.

The volume of users combined with large quantities of network traffic continue to pose issues (Kavanaugh et al., 2012). Techniques for regulating online social network content typically fall within one of two categories, proactive or reactive. Proactive measures address content before and as it happens and attempt to prevent its appearance on a given platform in the first instance. Online filters and keyword matching are methods for highlighting posts of a particular type and prevent certain forms of language from being submitted (Bekkers et al., 2013). Yet the speed of linguistic developments mean that these methods can only serve a limited purpose and may quickly become ineffective as new offensive terms or phrases are developed or ways to circumvent their use are discovered (through the use of punctuation, special symbols to break up the plain text meaning of a word). The application of sentiment analysis techniques allow for the identification of content-specific messages (Ceron et al., 2014) where the utilization of such methods may also support the automated recognition of offending messages. Social media platforms have also taken steps to encourage users to be proactive about reporting incidents online as opposed to waiting for a response from the network itself, introducing the notion of self-policing and user-regulation. Facebook have an inbuilt reporting system (Facebook, 2016e) with similar process witnessed on other platforms such as Twitter (2016d) and Instagram (2016d). Yet despite such methods, it remains arguable that the complete prevention of abuse is unachievable. Regardless of form, where content is posted that reaches its intended target (i.e. a victim's account) in breach of regulations, a reactive response must be formed in order to reprimand those responsible.

Where message content breaches platform policies or legislation, it may be deemed necessary to identify and prosecute the individual responsible for the post. This is particularly necessary in numerous cases including those of online harassment and threatening behaviour where in the UK, the circumstances of the case satisfy the test defined in the Code for Crown Prosecutors (Crown Prosecution Service, n.d.). The test is twofold where first evidential sufficiency must be achieved ('a prosecutor must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction'), before consideration must be given as to whether a prosecution is in the public interest. Before this test can be implemented, consideration must be given as to whether there is sufficient evidence available allowing the physical poster of any message content to be identified in the first instance. This can be a difficult process, and one where success is subject to the governance and guidelines of the platform from which the abusive content took place. In many circumstances, there is insufficient data available to identify account holders, hindering effective law enforcement investigation. In absence of the ability to identify an offender, there can often be no legal case to proceed with. On many

Please cite this article in press as: Horsman, G., A survey of current social network and online communication provision policies to support law enforcement identify offenders, Digital Investigation (2017), http://dx.doi.org/10.1016/j.diin.2017.03.001