Digital Investigation 13 (2015) 80–93

Contents lists available at ScienceDirect

Digital Investigation

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

An investigation of anonymous and spoof SMS resources used for the purposes of cyberstalking

Graeme Horsman*, Lynne R. Conniss

Northumbria University, Faculty of Engineering and Environment, Pandon Building, Camden Street, Newcastle-upon-Tyne, NE2 1XE, United Kingdom

ARTICLE INFO

Article history:
Received 22 August 2014
Received in revised form 30 March 2015
Accepted 1 April 2015
Available online 16 May 2015

Keywords:
Digital forensics
Mobile forensics
Cyberstalking
Online harassment
Anonymous SMS
Spoof SMS
Flash SMS
Harassment legislation

ABSTRACT

In 2012, the United Kingdom actively sought to tackle acts of stalking through amendments to the Protection from Harassment Act 1997. Now, not only is stalking a recognised criminal offence, acts associated with stalking behaviour have finally been properly defined in legislation. Further, the role of technology in digital stalking offences, frequently termed as acts of cyberstalking, has been duly highlighted. The prosecution of such cyberstalking offences is reliant on the forensic analysis of devices capable of communication with a victim, in order to identify the offender and evidence the offending content for presentation to a court of law. However, with the recent proliferation of anonymous communication services, it is becoming increasingly difficult for digital forensic specialists to analyse and detect the origin of stalking messages, particularly those involving mobile devices. This article identifies the legal factors involved, along with a scenario-based investigation of sample anonymous and spoof SMS (Short Message Service) messages, documenting the evidence that remains on a victim's handset for the purpose of locating an offender, which often may be minimal or non-existent.

Introduction

Acts of stalking can have severe and debilitating effects on a victim, leading to anxiety, depression, mental disorders and fear for personal security (Marcum et al., 2014). Recently, there has been an acknowledged and significant increase in officially recognised acts of stalking and harassment (Samuels, 2013) and it is suggested that in the United Kingdom (UK), around one in five women and one in ten men over the age of 16 in have been affected (Smith et al., 2011). Maple et al. (2011) highlight figures from the UK Crown Prosecution in year prior to publication which indicated "*33% of stalking incidents were by e-mail, 32% by text message and a further 8.4% were through social networking sites*". Further, a survey carried out by the European Union Agency for Fundamental Rights (2014) indicated approximately 9 million women had experienced acts of stalking in the EU within a 12 month period directly prior to the survey, with those aged between 18 and 29 more likely to experience cyberstalking.

Whilst there is no strict legal definition of stalking (CPS, 2014), the act of stalking in general terms involves "*harassing or persecuting (someone) with unwanted and obsessive attention*" (Oxford Dictionaries, 2014) which can be perpetrated both physically and via remote means such as the use of digital devices and phone calls, which are now commonly used throughout society. For example, a stereotypical view of stalking may once have conjured visions of individuals being followed through darkened alleyways, yet now, this type of offence is frequently committed online or using digital mobile devices which led to the introduction of the term cyberstalking. A non-physical offence, cyberstalking can be defined as the unsolicited

* Corresponding author.
E-mail addresses: g.horsman@northumbria.ac.uk (G. Horsman), lynne.conniss@northumbria.ac.uk (L.R. Conniss).

http://dx.doi.org/10.1016/j.diin.2015.04.001
1742-2876/

use of electronic communications for the purpose of causing fear and distress to another (Roberts, 2008). As with traditional stalking characteristics, the offender may be known or unknown to the victim. There are also traits comparable to cyberbullying and online trolling since the person behind the acts seeks to acquire an emotional response from their intended victim (Cavezza and McEwan, 2014). Although cyberstalking allows offenders to potentially target victims on a large geographical scale, Casey (2011) notes that in some cases, an offender's role may escalate to physical acts, which would only be likely to occur if the intended victim was within a feasible travel range for the perpetrator.

This paper presents an analysis of the recent addition of stalking legislation in the UK, reflecting on how this is situated with sample legislation in other parts of the European Union (EU) and exploring the impact technology provides for opportunities of cyberstalking. A scenario-based investigation is then presented, focusing on the forensic analysis of anonymous and spoof SMS (Short Message Service) resources that could be utilised to execute digital stalking offences.

Stalking and harassment legislation in the UK

Prior to the introduction of stalking as a recognised offence in the UK, activity which may be perceived as stalking could only be tackled under the existing offence of harassment defined in Section 1 of the Protection of Harassment Act (PHA) 1997 (MacEwan, 2012). Under PHA Section 1, an act amounts to harassment if the alleged offender 'knows or ought to know their conduct amounts to harassment' and in turn, 'the reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other'. Although acts of stalking, and specifically, cyberstalking, may fall within this classification of harassment, no direct and clear guidance was previously available for distinguishing behaviours which constituted these acts. The PHA 1997 was introduced as a method of protecting individuals against activities, which were not illegal per se, yet caused the intended target fear and distress (Home Office, 2011a).

Although the 1997 Act did not directly tackle stalking, and, in particular, acts of cyberstalking, the Home Office stated that it was established with these purposes in mind (Home Office, 2011a). However, subsequent consultation responses noted concerns regarding the ability to directly address the acts of cyberstalking via the PHA 1997, suggesting that the Act was failing to protect victims, as was originally intended (Home Office, 2011b). In 2012, via the Protection of Freedoms Act 2012 s.111, the PHA was amended to include offences related to stalking (Sections 2A and 4A). Of particular interest, the PHA now proceeds to directly define acts under Section 2A(3), which are associated with stalking as follows:

(a) following a person;

(b) contacting, or attempting to contact, a person by any means;
(c) publishing any statement or other material;
  (i) relating or purporting to relate to a person, or;
  (ii) purporting to originate from a person;

(d) mosnitoring a person's use of the Internet, email or any other form of electronic communication;
(e) loitering in any place (whether public or private);
(f) interfering with any property in the possession of a person;

(g) watching or spying on a person.

With more clearly defined legal guidance, digital forensic practitioners can henceforth seek to play a more prominent role in supporting the enforcement of stalking offences under the revised PHA. Within the UK, prosecution must prove beyond reasonable doubt that a defendant has committed the crime in question. Arguably, digital evidence will play a key role in relation to establishing actions falling under Sections 2A(3) (b), 2A(3) (c), 2A(3) (d) and 2A(3) (g).

Although a relatively new concept, cyberstalking has also been widely adopted in U.S. legislation as a standalone offence (Hazelwood and Koon-Magnin, 2013). In Europe, the formal recognition of cyberstalking as a distinct offence varies with less than half of the member states reported to maintain legislation directly targeting stalking alone (including the likes of Austria, Belgium, Denmark, Germany, Ireland, Italy, Luxemburg, Malta the Netherlands, Poland, the UK), with only Australia, Belgium, the United States and the United Kingdom identifying a standalone offence of cyberstalking within domestic legislation (Wurm, 2013; van der Aa and Römkens, 2013). van der Aa (2011) state that many EU member states favour utilising existing stalking legislation for dealing with cyberstalking, rather than developing and implementing new legislation; however, Germany does go further by including telecommunication devices as a tool used for stalking in their legislation (Wurm, 2013).

The influence and role of digital communications

Technological advancements have been driven by consumer desire for better online services and facilities. This has resulted in a significant increase in the use of, and dependency on, technology and the Internet which in turn offers increased opportunities for multiple types of deviant behaviour, of which cyberstalking is one such example. Ease of online access and the proliferation of affordable devices used for electronic communication have facilitated potential opportunities for cyberstalking providing multiple mechanisms through which acts could be perpetrated (Maple et al., 2011). Further, social media networking services such as Facebook and Twitter afford access to a larger volume of potential victims (Sen, 2013). Stalkers often demonstrate a sustained obsession with their victim that can be stimulated by the ease of access to, and, the volume of personal information placed online (Casey, 2011).

The role the Internet has played in assisting the perpetration of stalking activities should not be underestimated since it creates a perfect environment for this type of