Investigating employee harassment via social media

Dr Mark Taylor (Corresponding Author)
Senior Lecturer
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool, L3 3AF
(email: m.taylor@ljmu.ac.uk)
(Tel: 0151 231 2215)

Dr John Haggerty
Senior Lecturer
School of Science and Technology
Nottingham Trent University
Burton Street, Nottingham, NG1 4BU
(email: john.haggerty@ntu.ac.uk)

David Gresty
Researcher
Centre for Computer Security, Audit, Forensics and Education
Queen Mary Court, University of Greenwich, London, SE10 9LS
(email: david.gresty@gmail.com)

Dr Natalia Criado Pacheco
Lecturer
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool, L3 3AF
(email: n.criadopacheco@ljmu.ac.uk)

Dr Tom Berry
Senior Lecturer
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool, L3 3AF
(email: t.berry@ljmu.ac.uk)

Peter Almond
MSc Student
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool, L3 3AF
(email: donpeteralmond@hotmail.com)

Purpose

To examine the process of investigation of employee harassment via social media in order to develop best practice to help organisations conduct such investigations more effectively.

Design / methodology / approach

Review of the technical, managerial, and legal literature to develop guidance for organisations conducting investigations of employee harassment via social media.

Findings

Organisations may not have effective procedures for the investigation of social media misuse in general and employee harassment via social media in particular. This paper provides guidance for organisations to conduct investigation of employee harassment via social media more effectively.

Originality / value

The paper consolidates the fragmented discussion of the investigation of social media misuse with regard to employee harassment via a literature review across technical, managerial and legal disciplines. The paper provides guidance to support organisations conducting investigations of employee harassment via social media more effectively.

Abstract

Previously the investigation of employee harassment within the workplace would typically have involved obtaining evidence regarding physical contact, verbal contact (face to face or via telephone) or written contact (via letters or notes or email) between a suspect and a victim. Social media has added a new avenue to the investigation of employee harassment that goes beyond the physical workplace and normal working hours. In this paper we examine the process of computer forensic investigation of employee harassment via social media and the legal aspects of such. In particular we examine employee harassment via social media in terms of the reporting of harassment, the computer forensic investigation process, the relevant UK legislation and its application, and discuss good practice guidelines for educating employers and employees regarding how to use social media in the workplace and beyond in an acceptable manner.

Keywords social media misuse

1. Introduction

Kaupins and Park (2011) stated that corporate social networking sites can provide employees and employers with considerable opportunity to share information. However, Van Laer (2013) commented that misuse of social media in the form of cyber harassment can have harmful effects on social media users, such as emotional distress. Employers, and employees, as well as the legal system, are being affected by the growth and proliferation of social media, and the challenges and difficulties presented by the use of social media in the modern-day workplace (Lakhani, 2013; Eivazi, 2011; Kierkegaard, 2010). Courts as well as legislative bodies are beginning to address the legal issues caused by inappropriate social media use in the workplace

(Cavico et al, 2013, Jacobson, 2013, Geach, 2009). Organizations are becoming aware of the problems that may occur when employees use social media inappropriately both within and outside the physical workplace, and within and outside normal working hours (He, 2012; McDonald and Thompson, 2015; Garrie and Wong, 2010). In addition, the actual posting of material concerning employee harassment to social media sites could take place almost anywhere due to the availability of social media on tablets and smartphones. Employee harassment via social media has led to cases of unfair, constructive and summary dismissals and problems for both employers and employees that need to be addressed as employees' use of social media continues to grow and is likely to do so in the future (Khan et al 2011). Field and Chelliah (2013) commented that employers need to get to grips with the risks associated with social-media use by employees. Employers need to investigate alleged employee harassment via social media since the alleged harassment could contravene company policies, UK law, potentially leading to employment tribunals, court cases and the negative publicity associated with cases of harassment.

Lakhani (2013) discussed three categories of social media information: private information in the form of instant messages, emails, photo albums and contact information; semi-private (or semi-public) information available to a select group of 'friends' or wider networks such as 'friends of friends'; and public information such as text, media or other information available to the general public. Employees may consider that off-duty conduct on social media outside the physical workplace is unrelated to the employer's responsibility with regard to workplace conduct.

Morrison (2104) suggested that employers should communicate in a clear and unambiguous fashion the standard of behaviour expected from their employees with regard to social media usage. Depending on the extent of social media use within the workplace, it might be appropriate for employers to consider giving relevant employees training in how not to find themselves on the wrong end of a social media-induced harassment claim. Ideally employers should implement an explicit social media policy, that may form part of a more generic internet and computer usage policy. Such a policy might include the employer's right of access to content on its own computing hardware, so that if suspected harassment might have been conducted via a corporate device, the employer would have a general right of access. For an employer investigating employee harassment, social media may provide current digital evidence of employee harassment. In addition, archived data could also potentially be requested from the social media provider, however, this might typically only be available to a police investigation if the employee might consider taking the case to court.

Piotrowski (2012) commented that although there has been a proliferation of research into workplace bullying, there has been only limited research into the incidence and impact of cyberbullying in the workplace. Dempsey et al (2011) argued that cyber technology such as social media has provided new tools for peer aggressors. Carter (2013) commented that cyber bullying on social networking sites goes beyond the boundaries of time and space that distinguishes cyber bullying from more traditional forms of bullying. In some circumstances, it may sometimes be difficult to determine what may constitute harassment via social media in the workplace. For example, Mainiero and Jones (2013a) discuss the difficulties arising when workplace romance may stray into sexual harassment via social media, and also discuss potential guidelines for organizations to adopt relating to such use of social media (Mainiero and Jones, 2013b).

The unique contribution of the research reported in this paper is that it examines the computer forensic process and legal aspects of the investigation of employee harassment via social media in order to provide management guidance for corporate investigations of such. In addition, good practice guidelines are proposed to provide organizations with policy and education approaches to attempt to avoid such misuse of social media by employees. It is important that organizations investigate alleged employee harassment via social media in a timely and forensically rigorous manner. This is necessary in order to provide digital evidence of an appropriate standard for any internal corporate disciplinary proceedings, employment tribunal or court case, for example, a criminal or civil case concerning offences contrary to the UK Protection from harassment Act 1997 (PHA, 1997) that might ensue.

2. Literature review

2.1 Employee harassment

Employees should be protected from harassment in the workplace by a combination of employer's policies and legislation. Organizations should have a staff bullying and harassment policy that clarifies what is deemed to be bullying and harassing behaviour, and that provides guidance for the procedures to be followed in cases of alleged bullying or harassment. Bullying and harassment can create serious problems for an organization including: poor performance, lost productivity, absence, resignations, damage to company reputation and in severe instances, could lead to tribunal and other court cases and payment of unlimited compensation (UK Gov, 2015).

Organizations should treat all instances of alleged employee harassment in a similar manner, whether the alleged harassment is face to face, in written form, or via a digital medium. Harassment is commonly understood as behaviour intended to disturb or upset an individual that is repetitive. Examples of bullying or harassing behaviour may include: spreading malicious rumours, picking on someone, or regularly undermining a competent worker (UK Gov, 2015). Harassment relating to age, sex, disability, gender, marriage and civil partnership, pregnancy and maternity, race, religion or belief, or sexual orientation is unlawful under the UK Equality Act 2010 (EA, 2010). Typically, sexual harassment is one of the most common forms of workplace harassment in the UK (UK Gov, 2015). In order for workplace harassment or bullying to be established, there would typically need to be more than one incident that is intended to undermine, humiliate or injure the recipient. Workplace harassment may occur in various forms from discrimination to intimidation, bulling and stalking. Harassment via social media could take various media forms, including text, drawings, images, animations, and videos that by their content undermine, humiliate or injure the recipient directly, or do so through being viewed by others in the workplace.

2.2 Legislation relevant to employee harassment

The UK Protection from Harassment Act 1997 (PHA 1997) defines harassment as follows: "A person must not pursue a course of conduct (a) which amounts to harassment of another, and (b) which he knows or ought to know amounts to harassment of the other". Besides the UK Protection from Harassment Act 1997 (PHA, 1997) and the UK Equality Act 2010 (EA, 2010), other UK legislation that may apply to cases of employee harassment via social media includes the UK Malicious Communications Act 1988 (MCA, 1988) which might relate to sending electronic text or other articles with intent to cause distress or anxiety, the UK Communications Act 2003 (CA, 2003) which might relate to sending message that are of menacing character or

grossly offensive, and the UK Public Order Act 1986 (POA, 1986) which might relate to electronic communications that cause harassment, alarm or distress. There are overlaps in UK law that could apply to harassment via social media, however, these have been deemed necessary to provide for different circumstances (UK Parliament, 2014). In most cases the UK Equality Act 2010 (EA, 2010) and the UK Protection from Harassment Act 1997 (PHA, 1997) would typically be the most relevant legislation to cases of employee harassment. For large multi-national organizations, employee harassment could potentially occur across jurisdictional boundaries (ACPO, 2009), in which case other legislation besides UK legislation could apply. Whilst there is a variety of UK legislation that could apply to employee harassment via social media, it has not been deemed necessary to create new UK legislation to specifically address this particular type of harassment (UK Parliament, 2014).

2.3 Investigating employee harassment via social media

The acquisition of digital evidence relating to alleged employee bullying or harassment via social media should be performed by a competent computer forensic specialist familiar with appropriate computer forensic software tools (for example Encase (Encase, 2014) or FTK (FTK, 2014)) and follow appropriate procedures for computer forensic investigation (O'Floinn, and Ormerod, 2012) to ensure that the digital evidence obtained would be of an appropriate standard and would be admissible in court if required. Different standards of proof would be required for criminal as opposed to civil proceedings. Ideally a procedure of a similar standard to the UK Association of Chief Police Officers (ACPO) Good practice guide for digital evidence (ACPO, 2012) should be used. At present there do not appear to be any guidelines in widespread use specifically aimed at the process of obtaining and analyzing digital evidence from social media (Taylor et al, 2014).

The main research questions examined in this paper were:

- How should employee harassment via social media be reported?
- How should computer forensic investigation of employee harassment via social media be undertaken?
- How should digital evidence of employee harassment via social media be acquired?
- How should digital evidence of employee harassment via social media be reported?
- What are the legal aspects of investigating employee harassment via social media?

3. Procedures for investigating employee harassment via social media

3.1 Reporting of employee harassment via social media

Employee harassment via social media could include locating personal information about a victim, communicating with the victim, damaging the reputation of the victim, or tricking other social media users into harassing or threatening the victim (ACPO, 2009). Piotrokski (2012) commented that managers may not appreciate the full extent that cyber abuse may have on their employees, especially in terms of the potential legal liability of cyberbullying behaviours. Employers have a responsibility to ensure that employees have a workplace free from

discrimination, intimidation, bullying and harassment. Employees should report harassment to the organization at an early stage to prevent its escalation.

Previously the reporting of employee harassment to corporate management might typically have been done by the person being harassed. However, other employees may possibly have witnessed physical or verbal harassment in person, or possibly viewed written forms of harassment (letters left open to view, or possibly have been copied in to emails) and reported such to corporate management. In the case of social media, other employees may become aware of harassment via the social media that occurs not just inside, but also outside the physical workplace and outside normal working hours as well (Carter, 2013).

In theory, harassment via social media might be witnessed by more employees than harassment via other more physical means and therefore the likelihood of reporting harassment to corporate management by someone other than the subject of the harassment might be higher. Any reporting of alleged employee bullying or harassment should be done in accordance with the organization's policy for such, assuming that such a policy is in place. Typically alleged employee harassment would be reported to the employee's line manager, unless of course the line manager was associated with the harassment, in which case the alleged harassment might typically be reported to the line manger's manager. Alternatively in some instances, the harassment might be reported to the human resource department in the organization (if such exists), or possibly to a union representative within the organization (if such exists). Some employees might also report the bullying or harassment to the social media provider.

3.2 Corporate computer forensic investigation process for employee harassment via social media

The purpose of a computer forensic investigation of alleged workplace bullying or harassment via social media would be to obtain reliable digital evidence to support (or refute) the alleged bullying or harassment of an employee by other employees. The computer forensic investigation process should be conducted in a forensically sound manner, ideally to a standard similar to that of the UK Association of Chief Police Officers Good Practice Guide for Digital Evidence (ACPO, 2012). Such digital evidence would be required for any possible internal corporate disciplinary panel, employment tribunal or court case that might follow.

3.3 Timeliness of investigation

Given the ease of change of social media content (since social networking applications are intended for mass use) it would be appropriate to acquire relevant digital evidence as soon as possible following the reporting of the alleged employee bullying or harassment via social media. Relevant digital evidence may be obtained from relevant web pages relating to the social networking application used, computing devices used by the alleged suspect and victim, and possibly from archives maintained by the social media provider if required for a police investigation. It is important to remember when searching for digital evidence in such cases that employee bullying and harassment via social media (unlike other forms of bullying and harassment) can occur outside the physical workplace and outside normal working hours and via a range of physical computing devices.

3.4 Conducting the investigation

Computer forensic investigation of employee harassment via social media would typically be carried out internally by the organization. The UK Regulation of Investigatory Powers Act 2000 (RIPA, 2000) would cover the extent to which organisations could monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications systems. The employer should only monitor where the employer reasonably believes that the sender and intended recipient have consented to the interception, or without consent in order to prevent crime, protect the business or comply with financial regulations (ACAS, 2015).

If the harassment involved racial, gender, sexual orientation or disability discrimination in contravention of the UK Equality Act 2010 (EA, 2010), then a police investigation might possibly ensue. The UK Protection from Harassment Act 1997 (PHA, 1997) might apply in cases of repeated and severe bullying. There would be no legal requirement for the organization to report such matters to the police. However, if the subject of the harassment felt that the internal corporate investigation and subsequent outcomes were insufficient, then they might take legal action at an employment tribunal, or other courts.

3.5 Acquiring digital evidence

Digital evidence relating to suspected employee harassment via social media can potentially be acquired from a variety of sources by the computer forensic investigator. In the first instance, there would be an attempt to obtain digital evidence from relevant social media web pages. However, the contents of such may change quickly, and therefore the evidence should ideally be gathered as soon as is practicable after the alleged harassment is reported to the organization. Approaches for social media misuse investigations within organizations are typically not well defined and the approach used would also depend upon the social media involved. For example, it might be difficult to prove that a particular employee actually posted material concerning the alleged harassment if the social media service used did not supply Internet Protocol (IP) address or billing information (Taylor et al, 2014). O'Floinn and Ormerod (2012) commented upon the importance of the quality of digital evidence from social media and the need for adherence to appropriate procedures for the acquisition of digital evidence relating to social media use to ensure admissibility.

Potential digital evidence of employee harassment might be conveniently recovered by visiting the relevant web pages of the social media website and taking copies of the relevant content. The alleged harassment may have occurred on multiple social media platforms, each of which would need to be investigated. All activities undertaken by the computer forensic investigator should be recorded in a log, in order to provide an audit trail of the investigation process. For example, the computer forensic investigator should record the address of the website or the specific web page within the website that contained the potential digital evidence relating to the alleged employee harassment. The copying of digital evidence from a social media website should ideally be recorded using video capture software. This would record a visual representation of the content of the relevant web pages when they were visited by the computer forensic investigator. Alternatively the web pages could be saved as screenshots. The web pages themselves should also be saved, in order that the program code from the web pages is also recorded, as the source code might also be relevant to the investigation.

Given that social media content can in some instances be highly transient, it might in some circumstances be appropriate that the individual within the organization to whom the alleged harassment is reported (or even the employee actually reporting the alleged harassment) be

asked to make a copy of the relevant social media content by whatever means they have at their disposal. This would of course limit the reliability of the digital or printed evidence for any subsequent corporate disciplinary hearing, employment tribunal or court case. A copy of a web page or screen print made by a non-expert could be used as evidence, however, if it were presented by a non-expert then no expert interpretation of the content could really be made. If such evidence were to be presented by a computer forensic expert, the onus would be on the computer forensic expert to explain the implications and limitations of a non-expert having saved a web page rather than through a forensically sound capture process.

Additional evidence could then potentially be obtained from the suspect's computing device. However, the suspect could have used a variety of devices including personal computers, tablets, smartphones or even computer games consoles to post the material relating to alleged harassment to a social media site. In addition, not all such computing devices might be accessible to the corporate investigation team since they could belong to the employee suspected of harassment. The victim's computing device could be another source of evidence. However, this also might not be available to the corporate computer forensic investigation team if it belonged to the employee. The social media service's server computers and relevant Internet service provider's server computers could provide digital evidence, however, such would not typically be available for an internal corporate investigation, only for police investigations, and even in such cases jurisdictional issues might apply if the servers were located in another country.

Locating relevant social media artefacts related to suspected employee harassment on a computing device involves identifying the social networking software that was used, the operating system deployed on the computing device, and the Internet browser used. Specific computer forensic software tools aimed at gathering digital evidence from social media applications could potentially make the process of evidence acquisition easier for organizations investigating alleged employee harassment via social media.

3.6 Types of social media artefacts

Different types of social media artefacts of interest to the investigation may be located in different directories and files on the computing device in question. For example, Facebook (Facebook, 2015) artefacts could be located in the browser cache, unallocated clusters or system restore points of a computer. The different types of Facebook artefacts that might be relevant to an investigation of employee harassment could include: Facebook comments artefacts stored in HTML format in temporary Internet files or web cache; Facebook message / chat artefacts stored as JavaScript Object Notation (JSON) text in the pagefile.sys or hiberfil.sys files on a Windows computer; Facebook pictures stored in temporary Internet files or web cache; Facebook web page fragments stored in HTML format in temporary Internet files or web cache; and Facebook URLs stored in any web related (browser) artefact that references Facebook URLs.

Twitter files (Twitter, 2015) stored on a computing device that may be of interest to an investigator contain data such as the Twitter application's user information including the user name, URL link pointing to the user's profile picture, tweets posted by the user, and the timestamps of posted tweets. Stored Twitter files can also contain records of people followed by the user, their user names, information taken from their profile pages, URL links pointing to their profile pictures, tweets posted by them, and the timestamps of their posted tweets (Al-Mutawa et al, 2012).

3.7 Searching for relevant digital evidence

When acquiring digital evidence relating to alleged employee bullying or harassment via social media, a starting point for searching for such digital evidence might be the particular dates (and possibly times) that the alleged bullying or harassment took place as reported by the person (or persons) informing corporate management of such. As well as searching for textual, image and video artefacts relating to one particular reported incident, for cases of bullying or harassment it might typically be necessary to search for digital evidence concerning other related instances of bullying or harassment. In terms of search strategies for relevant evidence relating to employee harassment via social media, the computer forensic investigator might search for materials concerning the specific individuals or groups with which the suspect has communicated via social media, the specific timeframes within which social media communications took place, the patterns of communication via social media, the artefacts relating to one or possibly more social networking applications that were used and the types of media used in the communications including text, video or image (Taylor et al, 2014).

In addition to searching for digital evidence relating to alleged bullying or harassment of a victim by a suspect via social media, it would also be useful to acquire the content of the responses or actions of the victim regarding the suspect via the social media. In some cases there may be counter-allegations relating to the victim by the suspect. There is a possibility that the employee making a complaint may be doing so as a means to cause harassment to the alleged suspect, or to confuse or negate any allegations against themselves (ACPO, 2009).

3.8 Reporting digital evidence

When reporting the results of the computer forensic investigation of alleged employee bullying or harassment via social media it would be useful to present a timeline of events, showing the actions and responses of the alleged perpetrator and victim, in order for the context of the alleged bullying or harassment to be understood. It may not always be the case that the alleged victim behaved in a completely blameless manner in any interactions involving the social media used. The computer forensic investigation report should contain a description of all the actions carried out by the computer forensic investigator, the computer forensic software tools used for the investigation, and include details of all the digital evidence acquired. This might include details of the social media web pages concerned, screenshots of their content, and the date and time accessed, and the directories and file names of relevant social media artefacts on given computing devices, and details of when such were created, last updated, and last accessed.

4. UK cases involving work related harassment via social media

One of the first cases of harassment via social media in the UK occurred in 2007. The case involved a postgraduate student working at the University of Kent's library. The postgraduate student was made the subject of a Facebook group calling for him to be assaulted by other students due to the postgraduate student's alleged harsh manner whilst working at the university library (BBC, 2007). More than 350 people joined the Facebook group which was called "For those who hate the little fat library man". The pages of the Facebook group contained offensive comments regarding the postgraduate student, and a picture of the student taken by one of the group members on a mobile telephone. The University of Kent condemned

the use of offensive and derogatory statements and alerted Facebook to the contravention of the company's code of practice. Facebook's terms of use state that members may not post material which could "intimidate or harass another". The Facebook group was shut down and the case did not proceed any further.

There have been a number of instances of employees being disciplined and dismissed due to harassment of other employees via social media, for example in a case heard by a Northern Ireland Industrial Tribunal, *Teggart v TeleTech UK Limited* [2012] NIIT 00704_11IT, a company employee (a customer services operative) made scurrilous comments about the sexual promiscuity of a work colleague in his free time and from his home computer. The colleague was excluded from the ensuing Facebook discussion, but later became aware of the discussion. The comments on Facebook included reference to the employer (TeleTech) and were read by Facebook friends including work colleagues, but not the female colleague mentioned. A complaint by the colleague's friend to the company management led to suspension and disciplinary proceedings against the employee making the inappropriate comments (Bryden and Salter, 2013). The company (TeleTech) concluded that the comments on Facebook amounted to gross misconduct and the employee was dismissed. The employee brought a claim in the Northern Ireland Industrial Tribunal for unfair dismissal and for violation of his human rights, however, the claim was dismissed.

5. Legal considerations of employee harassment via social media

Bryden and Salter (2013) commented that there is the risk that an employer could be found to be vicariously liable for harassment or bullying committed by an employee against another employee, which could be costly and cause vast reputational damage to the organization concerned. The victim of the harassment could potentially take a case of harassment to court under the UK Equality Act 2010 (EA, 2010), the UK Protection from Harassment Act 1997 (PHA, 1997), or possibly the UK Malicious Communications Act 1988 (MCA, 1988), the UK Communications Act 2003 (CA, 2003), or the UK Public Order Act 1986 (POA, 1986).

When investigating suspected employee harassment via social media within an organization it is important to adhere to the security principle of the UK Data Protection Act 1998 (DPA, 1998) with regard to any personal data encountered during the investigation. Any personal data obtained in the course of investigating suspected employee harassment via social media should not be accessible to those outside the internal investigation team. Bryden and Slater (2013) and McGoldrick (2013) suggested that postings relating to harassment on personal social media in free time from personal computing equipment would not generally be covered by a reasonable expectation of privacy (under Article 8 of the European Convention of Human Rights), and that freedom of expression defences (under Article 10 of the European Convention of Human Rights) are not likely to succeed when personal comments relating to harassment are made against an individual (in this case a work colleague).

6. Employer policies regarding employee use of social media

It would be useful for employers to have explicit policies regarding the use of social media in the workplace (ACAS, 2015) and in particular with regard to activities that could be deemed to be harassment. The organization should communicate the standards of behavior expected from employees regarding the use of social media in a clear and unambiguous manner to all employees of the organization. This could possibly take the form of a specific employee social

media usage policy that describes what is considered to be acceptable social media usage by employees. This should include the use of social media by employees both within and outside the workplace. Outside the workplace would include both physically outside the workplace and outside normal working hours, and also cover employees' use of their own personal computing devices for social media. Other than a specific social media usage policy, organizations might include guidelines for acceptable social media usage by employees within a more generic company internet or computer usage policy. It would be appropriate for employees to be made aware of the relevant policy, and for a record of their acceptance of the policy to be retained by the organization. Ideally training for employees regarding the acceptable (and unacceptable) use of social media should be provided by the organization.

The organization's policy on social media usage should make clear to employees that personal blogs, Facebook (Facebook, 2015), Twitter (Twitter, 2015) or any other social media websites have clear disclaimers that the views expressed by the author (employee) are theirs alone and do not represent the views of their employing institution. Personal social media accounts should not contain anything that might suggest that the owner is acting in an official capacity with regard to their employing organization. The policy should also remind employees that they may be legally liable for anything posted online, at all times, in or out of working hours, and that all actions captured via images, videos, posts or comments online can reflect on the organization. The organization's policy on social media usage should also inform employees of the possible outcomes from inappropriate use of social media including suspension and dismissal.

Employees with their own personal profile on a social media website should make sure that others cannot access any content, media or information from that profile that the employee would not be happy for other employees to have access to and might undermine their position as an employee. Employees should consider changing the privacy settings on their social media profile so that only people that they have accepted as friends can see their content. In addition it would be practicable for employees to review who is on the 'friends list' on their personal profile.

7. Discussion

In this section we provide a framework that outlines the main issues associated with the investigation of employee harassment via social media, and the possible actions that can be taken by practitioners and managers.

Framework for investigating employee harassment via social media:

Issues	**Actions**
Reporting of employee harassment via social media	Ideally an organisational policy regarding harassment should be in place, this should explicitly include how to report harassment (typically via a line manager).
Computer forensic investigation process	Any investigation should be undertaken in a forensically sound manner, ideally to a standard similar to the UK ACPO guidelines.
Timeliness of investigation	Digital evidence should be acquired as soon as possible following reporting, given the ease of change of social media content.

Conducting the investigation	Typically undertaken by appropriately trained internal IT staff (or possibly an outsourced agency).
Acquiring digital evidence	Digital evidence would typically be acquired via relevant web pages and computing devices owned by the organization in a forensically sound manner.
Types of social media artefacts	Different types of social media artefacts might need to be examined dependent upon the social media service used.
Searching for relevant digital evidence	Relevant timeframes, individuals and groups should be identified to aid the search for digital evidence.
Reporting digital evidence	A computer forensic investigation report should contain a description of all the actions carried out by the computer forensic investigator, the computer forensic software tools used, and the details of all the digital evidence acquired.
Legal considerations	Various UK legislation might apply to the investigation including the UK Equality Act 2010, the UK Protection from Harassment Act 1997, and the UK Data Protection Act 1998.
Employer policies regarding social media	Ideally the organisation should have an appropriate policy regarding employee use of social media.

The implications of the findings for practice are:

- Employees should be aware of how to report harassment via social media.
- Managers should be aware of how to investigate employee harassment via social media.
- It practitioners involved in the investigation of employee harassment via social media should be aware of the need to follow appropriate computer forensic investigation procedures, use appropriate computer forensic software tools, and report the results of the investigation in a thorough and professional manner, with due regard for all relevant legislation.

8. Conclusions

In this paper we have examined the nature of employee harassment via social media, the computer forensic process for investigating such, and the legal aspects of employee harassment via social media in order to provide management guidance for corporate investigations of such. Employers should ideally implement a workplace bullying and harassment policy and an explicit employee social media usage policy (that may form part of a more generic employee internet and computer usage policy). It is important that corporate management ensure that allegations of employee bullying or harassment are taken seriously and that appropriate

investigations of such allegations are conducted in a timely and professional manner with due regard to any staff bullying or harassment policy in place within the organization and all relevant legislation. Computer forensic investigation of suspected employee harassment via social media should be conducted in a timely and rigorous manner so that digital evidence relating to alleged employee harassment of an appropriate standard will be available for any internal corporate disciplinary proceedings, employment tribunal or possible court case, criminal or civil that may ensue.

References

ACAS (2015) ACAS social media and how to develop a policy http://www.acas.org.uk/index.asp?articleid=3381

ACPO (2009) Practice advice on investigating stalking and harassment, The Association of Chief Police Officers of England, Wales and N. Ireland, http://www.acpo.police.uk/documents/crime/2009/200908CRISAHO1.pdf

ACPO (2012) Good practice guide for digital evidence, Version 5, The Association of Chief Police Officers of England, Wales and N. Ireland, http://www.acpo.police.uk

Al-Mutawa, N., Baggili, I., Marrington, A. (2012) Forensic analysis of social networking applications on mobile devices, Digital Investigation, 9, 24-33.

BBC (2007) British Broadcasting Corporation Online. 2007. Fat library man bullied online. BBC News Online,23 July. DOI=http://news.bbc.co.uk/1/hi/england/kent/6912409.stm.

Bryden, C., Salter, M. (2013) Beware of the web: Legal Update Employment, The New Law Journal, 163, 7569, 163 NLJ 9.

CA (2003) UK Communications Act 2003, http://www.legislation.gov.uk

Carter, M. (2013) Third party observers witnessing cyber bullying on social media sites, Procedia – Social and Behavioral Sciences, 84, 9 July 2013, 1296–1309

Cavico, F., Mujtaba, B., Muffler, S., Samuel, M. (2013) Social Media and the Workplace: Legal, Ethical, and Practical Considerations for Management, Journal of Law, Policy and Globalization, 12, 1, 1-46.

Dempsey, A., Sulkowski, M., Dempsey, J., Storch, E. (2011) Has cyber technology produced a new group of peer aggressors?, Cyberpsychology, Behavior, and Social Networking, 14, 5, 297-302.

EA (2010) UK Equality Act 2010, http://www.legislation.gov.uk

Eivazi. K. (2011) Computer use monitoring and privacy at work, Computer Law and Security Review, 27, 5, 516-523.

Encase (2015) Encase software, http://www.guidancesoftware.com

Facebook (2015) Facebook, https://www.facebook.com/

Field, J. Chelliah, J. (2013) Employers need to get to grips with social-media risks: Two key policies required to cover all the bases, Human Resource Management International Digest, 21, 7, 25-26

FTK (2015) Forensic Toolkit Software,
http://accessdata.com/products/computer_forensics/ftk

Garrie, D., Wong, R. (2010) Social networking: opening the floodgates to personal data, Computer and Telecommunications Law, 6, 167-175.

Geach, N. (2009) Regulating Harassment: Is the law fit for the Social Networking Age?, Journal of Criminal Law, 73, 3, 241-257.

He, W. (2012) A review of social media security risks and mitigation techniques, Journal of Systems and Information Technology, 14, 2, 171-180.

Jacobson, W., Tufts, S. (2013) To post or not to post: employee rights and social media, Review of Public Personnel Administration, 33, 1 84-107.

Kaupins, G. Park, S. (2011) Legal and ethical implications of corporate social networks, Employee Responsibilities and Rights Journal, 23, 2, 83-99.

Khan, S., Moores, R., Weal, M. (2011) Social Media on the Job: An exploration of the potential legal consequences of employees' social media activities during the course of employment, In Proceedings of ACM Web Science 2011 Conference, Koblenz, Germany, 14 - 17 June 2011.

Kierkegaard, S. (2010) Twitter thou doeth? Computer Law and Security Review, 26, 6, 577-594.

Lakhani, A. (2013) Social networking sites and the legal profession: Balancing benefits with navigating minefields, Computer Law and Security Review, 164-174.

Mainiero, L., Jones, K. (2013a) Sexual harassment versus workplace romance: social media spillover and textual harassment in the workplace, Academy of Management Perspectives, 27, 3, 187-203.

Mainiero, L., Jones, K. (2013b) Workplace Romance 2.0: Developing a Communication Ethics Model to Address Potential Sexual Harassment from Inappropriate Social Media Contacts Between Coworkers, Journal of Business Ethics, 114, 2, 367-379.

MCA (1988) UK Malicious Communications Act 1988, http://www.legislation.gov.uk

McDonald, P., Thompson, P. (2015) Social media(tion) and the reshaping of public/private boundaries in employee relations, International Journal of Management Reviews, DOI:10.1111/ijmr.12061

McGoldrick, D. (2013) The limits of freedom of expression and social networking sites: A UK perspective, Human Rights Law Review, 13, 1, 125-151.

Morrison, T. (2014) Private eye: Legal Update Data Privacy, The New Law Journal, 164, 7599, 164 NLJ 14.

O'Floinn, M., Ormerod, D. (2012) Social networking material as criminal evidence, Criminal Law Review, 7, 486-512.

PHA (1997) UK Protection from Harassment Act 1997, http://www.legislation.gov.uk

POA (1986) UK Public Order Act 1996, http://www.legislation.gov.uk

Piotrowski, C. (2012) From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations, Organization Development Journal, 30, 4, 44-53.

RIPA (2000) UK Regulation of Investigatory Powers Act, http://www.legislation.gov.uk

Taylor, M., Haggerty, J., Gresty, D., Almond, P., Berry T. (2014) Forensic investigation of social networking applications, Network Security, 11, 9-16.

Twitter (2015) Twitter, https://twitter.com/

Teggart v TeleTech UK Limited [2012] NIIT 00704_11IT

UK Gov (2015) Workplace bullying and harassment, https://www.gov.uk/workplace-bullying-and-harassment

UK Parliament (2014) UK Parliament, Communications Committee, Social media and criminal offences, Social media and the law http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm

Van Laer, T. (2013) The means to justify the end: Combating cyber harassment in social media, Journal of Business Ethics, 18, 2, 185-200.