Forensic investigation of social networking applications

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)

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

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)

Forensic investigation of social networking applications

Abstract

Social networking applications such as Facebook, Twitter and Linkedin may be involved in instances of misuse such as copyright infringement, data protection violations, defamation, identity theft, harassment, and dissemination of confidential information and malware that can affect both organizations and individuals. In this paper we examine the computer forensic process of obtaining digital evidence from social networking applications and the legal aspects of such. Currently there do not appear to be commonly available guidelines for organizations aimed specifically at the computer forensic process of investigation of social networking applications.

Keywords Forensic investigation social networking applications

1. Introduction

Social networking applications such as Facebook, Linkedin, MySpace and Twitter provide facilities including email, blogging, instant messaging and photo sharing for social and commercial exchange[1]. There has been a rapid growth in the use of social networking applications by both individuals and organizations[2,3]. An increasing number or organizations use Facebook and Twitter as part of their marketing campaigns[4,5]. Although social networking applications are mainly used for personal purposes, some organizations actively encourage their employees to use social networking applications within the work environment to potentially improve productivity via enhanced information sharing above and beyond the corporate network[6,7]. Social media can provide employees with formal and informal ties to information sources both within and beyond organizational boundaries[8]. However, some organizations might not fully appreciate the potential for misuse that social networking applications may provide[9]. If organizations do allow employees to use social networking applications within the work environment then it would be prudent to set out guidelines for such in the organization's computer usage policy[10, 11], to ensure that employees are provided with explicit guidance regarding the use of social media in the workplace. Morrison[12] commented that it is crucial for all employers to make clear the standards that are expected of their employees in relation to not only the use of corporate social media account, but also employees' own accounts.

Misuse of social media may occur in many different forms, from defamation of individuals, to nurses violating patient rights through misuse of social media[13] and data loss occurring to organizations resulting from inappropriate use of social media[14]. Forensic investigation of social media may be required for a variety of different purposes, from gathering evidence for use in a criminal trial[15] to use in corporate disciplinary panels for employees that have breached company policy[16]. Moore[17] commented that complaints originating from social media make up at least half of a front-line police officer's work according to the head of the UK College of Policing.

There do not appear to be any commonly used guidelines specifically relating to the computer forensic investigation of social networking applications[18,19]. The UK Association of Chief Police Officers' (ACPO) good practice guide for computer-based electronic evidence[20] provides a framework for UK police forces undertaking computer forensic investigations, and would be a practical starting point for organizations intending to undertake a forensic investigation of social networking application misuse. UK organizations may in some cases have limited guidance for internal computer forensic investigations[21], which could undermine the integrity of any digital evidence obtained during such an investigation. O'Floinn and Ormerod[22] commented that the use of evidence from social networking sites in criminal trials has become commonplace.

2. Computer forensic procedure for the investigation of social media

Typically, an individual, employee, or police officer may encounter suspected misuse of a social networking application (or details relating to a suspected criminal act) and then report such suspected misuse to the relevant authority (either their manager in an organization, or the local police force).

2.1 Scope of the investigation

Initially digital evidence might be obtained from the web pages of the social networking application containing the material associated with the suspected misuse, assuming that these can be accessed (that is not on 'private' pages). In an organization, a next step might then be to obtain digital evidence from the employee's computer (or in a police investigation, the individual's computer) that might be involved in the suspected of misuse of the social networking application. In addition, it might be necessary to obtain digital evidence from the computer of the employees (or individuals) who were affected by such misuse. Given the number of computing devices that could potentially be used to update material on social networking applications (personal computers, laptop computers, tablets, mobile telephones, personal digital assistants and computer games consoles), it may be necessary to examine a range of computing devices that may have been used by in misuse of the social networking application. In instances involving police investigations a request might be made to the provider of the social networking application for the relevant digital data relating to suspected misuse. In some instances (for police investigations) the server computers supporting the social networking application might need to be forensically examined.

2.2 Digital evidence acquisition for computer forensic investigation of social media

In terms of the ease of acquisition of digital evidence from social networking applications, the following order of potential sources of acquisition might typically be adopted:

1) Relevant social networking application web pages (if such can be accessed). Significant changes may be made to a web page at any time from when the message or post was initially made, to the time when the investigator attempts to

make a copy of the page. For example, a victim might allege harassment on a Facebook web page where there is a message stating "I will see you soon!" and the icon of a firearm next to it. When the investigator accesses the page the person posting the message has changed their icon to be a bouquet of roses. The investigator has to be suitably knowledgeable and qualified to identify what elements are mutable, and where the necessary additional evidence of an offence can be found from other sources, such as:

2) The suspect's computing device(s) (assuming the suspect can be identified and located). The potential difficulty with acquiring digital evidence from this source (or sources) is that social media can be accessed across a variety of platforms from mobile phones, tablet computers, e-readers and traditional desktops both at both or work.

3) The victim's computing device(s). Unlike an email-based investigation, social media is essentially about publication, and future modification of the post or web page means that although the victim's machine can be useful for the investigation, service provider logs potentially provide the best evidence.

4) Typically social networking service's server computers and relevant Internet service provider's server computers would only be available for police investigations, whereas the other sources would typically be available for both internal corporate and police investigations.

Where an incident involves potential evidence displayed on a social media website the most convenient method of recovering the evidence may be to visit the website and take copies of the relevant content. The forensic investigator should record the address of the website, or the specific web page within the website. When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the forensic investigator is recorded in a log. The recommended method for copying a website is to visit the website and record the relevant web pages using video capture software so there is a visible representation of how they look when visited at the time. If video capture software is not available then the pages can be saved as screenshots. It is also advisable to follow this by capturing the web pages themselves either by using website copying software or saving the individual web pages. Copying the web pages themselves, as well as obtaining a visual record, means that the code from the web pages is also secured should that become relevant later.

If it appears likely that the evidence on the social media website might be lost by a delay in carrying out the above procedures then the person reporting the incident might be asked to make a copy of the evidence by whatever means they are capable of (either printing, screenshot or saving pages), alternatively this could be done by the person receiving the report of the incident. Before taking these steps every effort should be made to secure the services of a competent person to carry out this work as failing to capture the information correctly could have a detrimental impact on the investigation. Any initial save of a web page or screen print made by the non-expert may have to be produced as an exhibit. If is being produced by a non-expert then no expert interpretation

of the content is made. If subsequently that initial exhibit is relied on by an expert, the onus is on the expert to explain the implications and limitations of a non-expert saving a web page rather than a forensically sound capture.

For police investigations where there is difficulty in capturing the evidence by visiting the social media website it might be possible to make an official request to the owner of the website by whatever legal procedures are required within the jurisdiction. By making a request to the service provider hosting the website it may be possible to recover evidence of who has created the web page or posting. It is not unusual for details of the user such as name, address, phone number, email address, and alternative email address to be recorded by a social media host. However, account hijacking may have taken place, so typically the Internet Protocol address at the time of the alleged offense is still essential to cover the exculpatory circumstances.

When any user accesses the Internet they are allocated a unique address known as an IP address and their Internet Service Provider (ISP) keeps logs of the times and dates and the identity of the user allocated any IP address. When a user visits a social media website and conducts some activity, for example logs on, or posts a message, it is likely that the user's IP address has been logged by the website. For police investigations it may possible to obtain copies of logs from websites if there is a requirement to see who has been active on a website. If the potential evidence is no longer available to be retrieved by any of the above means, it may be possible to recover evidence of the website contents from an end user device that has been used to view the website by conducting a forensic examination of the device.

2.3 Retrieving digital evidence relating to social media from different types of devices

Data resident on the hard drive of a computer involved in misuse of a social networking application, for example in the web cache, Internet history, log ins, username and password relating to the social networking application may be available using standard computer forensic procedures. However, digital data resident on social networking servers or Internet service provider's servers would be more problematic to access. Access to such data would be restricted to police investigations, and the investigators involved would have to apply to the social network services provider with appropriate authority.

Methods for corporate social networking applications misuse investigations are typically not well defined and would depend upon the social networking service involved, for example, how could it be proved that a particular individual posted a comment if the social networking service does not supply IP address or billing information. In addition, if an individual sent the post from their private mobile telephone, tablet or laptop computer, the organization would not have the authority to access this device.

The computer forensic investigation process might typically involve taking an image copy of the relevant storage device within the computing device (for example, the hard disk within a personal computer or laptop computer[23]). This is done in order to ensure that no corruption of the original data source could occur. An appropriate computer

forensic software tool such as FTK or Encase could then be used to search for relevant materials on the image copy. However, as Haggerty et al[24] discuss, existing computer forensic tools are designed to analyze evidence retrieved from storage media rather than examine data from online sources such as social media. This can be problematic as investigations involving social media have risen in prominence due to the information about a suspect that these data sources may yield to the forensic examiner.

Finding social media artefacts on a computing device will involve determining which social networking software was used, the operating system in use on the device, and the Internet browser used (e.g. Internet Explorer, Google Chrome or Firefox). Facebook artefacts, for example, could be located in the browser cache, unallocated clusters or system restore points of a computer. Categories of artefacts that might be of interest in an investigation concerning Facebook usage might include: Facebook message / chat artefacts that can be found as JavaScript Object Notation (JSON) text in the pagefile.sys or hiberfil.sys files on a computer running Windows; Facebook wall post / status update / comments artefacts that can be found in HTML in temporary Internet files or web cache; Facebook web page fragments that can be found in HTML in temporary Internet files or web cache; Facebook pictures that can be found in temporary Internet files or web cache, where the picture file name can indicate the Facebook user ID the picture belongs to; and Facebook URLs, a URL in any web related (browser) artefact that references Facebook URLs.

Examining data from mobile telephones and tablets can be somewhat more complex due to the variety of proprietary operating system in use on such devices. This can make extracting digital evidence from such devices problematic. In addition the different social media applications may store digital data in different formats and locations in the memory of the device. For example, on mobile telephones a database related to the Facebook application in stored in the phone's memory. The database stores data for each friend in the list including their names, ID numbers and phone number[25]. Twitter uses directories to store information about Twitter account data, attachments sent with Tweets, user names and date and time values[26]. MySpace uses an SQLite file to store the user name of the MySpace application, as well as comments that the user had posted along with timestamps[27]. Digital evidence relating to social media usage could be acquired by either a physical or logical method. However, with logical acquisitions, there is the possibility that data stored in slack space may be missed.

2.4 Software tools for acquiring digital evidence relating to social media

There are some specialist forensic software tools currently available such as Twitter investigator, and Facebook forensics and the MacForensicsLab social agent software tool that can scan particular types of computing devices, for example Apple Macs running the Apple Safari web browser for evidence of social network activity and can identify social networking web pages visited by the suspect. There are facilities in standard computer forensics software tools such as FTK and Encase that allow searches of browser history.

2.5 Analysing acquired digital data relating to social media

When investigating misuse of social media, approaches to searching for relevant evidence may concern:

- The specific individuals or groups with which the suspect has communicated via social media.
- Specific timeframes within which social media communication took place
- The patterns of communication via social media
- The artefacts relating to one or possibly more social networking applications that were used
- The types of media used in the communications e.g. text, video or image

Using an appropriate search approach can reduce the time and effort required to find either particular communication data, or to establish a particular pattern of communication as appropriate to the purposes of the investigation. For example, whether evidence would be required relating to one particular instance such as the communication of indecent material, or relating to on-going sustained harassment over a period of time.

2.6 Reporting of digital evidence from social media

After analysis of the digital data had been undertaken, then a report would typically be produced detailing the relevant evidence found and the process by which the evidence was obtained. This could then be used in a corporate disciplinary hearing or in a court case. Not only is social media evidence commonly available, but when presented may be highly influential with jurors. It is a familiar medium, and will often represent the very words typed or the images uploaded by defendants. The same would be true of such evidence presented during corporate disciplinary hearings.

Printouts of social media communications are considered documents, which may contain relevant evidence. Under section 133 of the UK Criminal Justice Act 2003 statements in documents can be adduced by providing either the document or a copy of the document or of the material part of it, authenticated in whatever way the court may approve. It is important that any reporting of digital evidence obtained from social media whether for court or for an internal corporate disciplinary hearing is done in a manner that allows for such to be authenticated to the satisfaction of the court or disciplinary hearing. Authentication issues relating to digital evidence from social media may relate to accuracy of the exhibit, proof pf authorship, identification of individuals in photographic evidence, and unfairly obtained evidence[28].

3. Legal aspects of forensic investigation of social networking applications

Any forensic investigation of misuse of social networking applications should follow the UK ACPO guidelines (if a police investigation) or guidelines of a similarly robust standard (if an internal corporate investigation) in order to attempt to ensure that any digital evidence obtained would be admissible in a court of law, or of an appropriately high standard for a corporate disciplinary panel.

For police investigations, the Crown Prosecution Service guidelines on prosecuting cases involving communications sent via social media provide guidance concerning the offences that are likely to be most commonly committed by the sending of communications via social media. The guidelines cover:

- Communications which may constitute credible threats of violence to the person or damage to property.
- Communications which specifically target an individual or individuals and which may constitute harassment or stalking within the meaning of the UK Protection from Harassment Act 1997.
- Communications which may amount to a breach of a court order. This can include offences under the Contempt of Court Act 1981, section 5 of the Sexual Offences (Amendment) Act 1992, and breaches of a restraining order or breaches of bail.
- Communications which may be considered grossly offensive, indecent, obscene or false.

The guidelines also cover the context in which any communication is sent which will be highly material, in particular with regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place. Social media access is ubiquitous and instantaneous, and banter, jokes and offensive comments are commonplace and often spontaneous. Communications intended for a few may reach millions. As stated in the civil case of *Smith v ADVFN* [2008] 1797 (QB)[29] in relation to comments on an internet bulletin board:

> *"... [they are] like contributions to a casual conversation (the analogy sometimes being drawn with people chatting in a bar) which people simply note before moving on; they are often uninhibited, casual and ill thought out; those who participate know this and expect a certain amount of repartee or 'give and take'."*

There may be jurisdictional considerations when undertaking an investigation of social network application misuse since social network application software usage may cross jurisdictional boundaries. Computers and computing devices used for social networking activities may be outside UK jurisdiction and therefore digital evidence from such devices may be more difficult to obtain. If any indecent images were found during an investigation of misuse of social networking applications within an organization, then the matter would have to be reported to the police. In addition any material found in an investigation of suspected social networking application misuse relating to potential money laundering would have to be reported to the police.

3.1 Data protection

When investigating computer misuse involving social networking applications it is important to be aware of the provisions of the UK Data Protection Act 1998 with regard to any personal data encountered during the investigation. Personal data obtained during a computer forensic investigation of social networking applications misuse should not be accessible to those outside the investigating team. Employees of an organization may violate the UK Data Protection Act 1998 if they upload personal data regarding other employees, or clients or customers of the organization via a social networking application[30]. If employees are encouraged or allowed to use social networking applications by their employer in the work environment, then under the security principle of the UK Data Protection Act 1998 the employer should apply appropriate technical and organizational security measures to protect personal data held by the organization[31]. When an organization or any individual acting for non-domestic purposes posts personal data via social media, they should comply with the UK Data Protection Act 1998. The same would apply to any personal data downloaded from social media that is used for non-domestic purposes.

The potential danger with social networking applications is that employees may view personal data in a different manner on social networking applications compared to corporate computer based systems[32]. For example, employees might be aware that personal data relating to colleagues or customers or clients should not be uploaded to the organization's website, or included in emails sent using the organization's email system, yet might disclose such information on a social networking application. For example personal details regarding illness or maternity of a colleague might be uploaded in a 'social' context whereas it might clearly be considered inappropriate by an employee to do so in a 'corporate' context via the company's intranet or email systems.

3.2 Regulation of Investigatory Powers Act

If on-going criminal activity involving misuse of social networking applications might be taking place within an organization, then potentially the organization or the relevant Internet service provider might be subject to the provisions of the UK Regulation of Investigatory Powers Act 2000 with regard to the monitoring of such activities or the collection and disclosure of communications data (data relating to the communication, for example, sender, recipient, date and time, rather than the actual content of the communication) for police officers or their agents.

3.3 Copyright

The culture of unauthorized sharing of copyrighted content is perceived as a major threat to copyright owners and content industries[33]. Social networking applications allow users to upload digital content which can then be accessible to other users of the social networking application. Such digital content uploaded by individuals might include images, audio and video files and ebooks. This is therefore a potential means of unlawful dissemination of copyrighted materials in contravention of the UK Copyright, designs

and patents Act 1988. Organizations such as FACT (Federation Against Copyright Theft) may contact organizations where employees may have infringed copyright via social networking applications. Under the UK Digital Economy Act 2010 Internet service providers will be obliged to send notifications to subscribers alleged by rights holders to be infringing copyright, and to monitor the number of notifications with which each subscriber is associated. Currently the provisions of The UK Digital Economy Act 2010 are not yet in force. The UK Digital Economy Act 2010 legislation will also oblige Internet service providers to make such notifications data available to rights holders on receipt of a court order[34].

3.4 Defamation

An employee (or organization) could be liable for defamation if comments were made regarding an individual (either another employee or an external individual) that might damage the reputation of that individual or the organization via a social networking application[35]. Employees may differentiate between comments made about an individual in a corporate email context compared to a social networking application context, and might be more likely to make inappropriate comments regarding individuals via social media[36]. Even if individuals were to retract statements made, there would still be a record of such statements on the social media. This can expose an organization to legal action as well as the individual, where some tacit authorization is given to use social media whilst at work[37].

3.5 Identity theft

Since social networking applications are aimed at individuals who wish to share personal information with others, they provide an ideal platform for identity theft by criminal gangs[38,39]. Although this might have adverse consequences for individuals, for example fraud or theft of bank funds, the same could apply to organizations if the criminals use the identity of an employee through information gained through a social networking application for illegal activities. This could involve misuse of the organization's computer systems or finances, if the information gained enabled access to such

3.6 Harassment

Employees who upload materials via a social networking application that could constitute harassment of another employee, customer or client of the organization[40] might face disciplinary proceedings by their employer, or possible prosecution, if such harassment infringed anti-discrimination legislation such as that relating to race, gender or disability[41]. In August 2009, Keeley Houghton became the first person to be convicted under the UK Protection from Harassment Act 1997 where one of the acts constituting the course of conduct in question was bullying pursued via a social networking site. A UK university student was jailed for 56 days for racist comments on Twitter in 2012.

3.7 Confidential information

Employees may inadvertently (or deliberately) disseminate confidential information relating to an organization if they were to publish information relating to the financial state of the organization, contracts, projects or products or services or other confidential information via a social networking application[42]. For example, it might appear harmless to an employee to publish information to work colleagues and friends via a social networking application stating that they are starting a new project with a given company, or developing a new type of product, or that the contract with a given company is not being renewed. However, it could not then be guaranteed how the colleagues and friends might then disseminate such confidential information via the social networking application. Such dissemination of confidential information is possibly more likely with regard to social networking applications such as Linkedin where users may be actively looking for employment, or may be in contact with individuals from competitor organizations.

3.8 Malware

The widespread use of social media provides a platform for the spread of malware such as computer viruses, worms, Trojan horses and spyware. Social engineering continues to be an increasing attack vector for propagation of malicious programs, and malware that specifically targets online social networks are on the rise[43]. Unlike corporate software applications which can potentially be more controlled and monitored by the organization, social networking applications may be more likely to expose users within an organization to malicious software.

4. Conclusions

In this paper we have examined the computer forensic process of obtaining digital evidence from social media, and the legal aspects of such. At present there does not appear to be commonly available guidelines for organizations specifically aimed at the computer forensic investigation of social networking applications. It is important that organizations that intend to undertake computer forensic investigations of social networking applications do so in a manner that does not undermine the integrity and admissibility of any digital evidence found relating to social networking application misuse, especially if such may be required for a criminal investigation by a police force.

Organizations should cover the use of social networking applications by employees in their computer usage policy. Some organizations may specifically ban the use of social networking applications by employees, and some may even advise against the use of such applications in any work related context for personal use (for example, teachers). For organizations that allow or support the use of social networking applications by employees in a work environment it would be advisable to explicitly state what would be deemed to be appropriate (and inappropriate) use of such applications by employees and the possible consequences of such. There is a wide variety of legislation that can potentially be relevant to misuse of social media in the workplace, and the forensic investigation of such.

References

1. Cavico, F., Mujtaba, B., Muffler, S., Samuel, M. (2013) Social Media and Employment- At-Will: Tort Law and Practical Considerations for Employees, Managers and Organizations, New Media and Mass Communication, 11, 25- 41

2. Purcell, R. (2010) Is that really me?: Social Networking and the right of publicity, Vanderbilt Journal of Entertainment and Technology Law, 12, 3, 611-639

3. Dennis, C., Morgan, A., Wright, L., Jayawardhena, C. (2010) The influences of social e-shopping in enhancing young women's online shopping behaviour, Journal of Customer Behaviour, 9, 2, 151-174.

4. Kozinets, R., De Valck, K., Wojnicki, A., Wilner, S. (2010) Networked Narratives: Understanding word-of-mouth marketing in online communities, Journal of Marketing, 74, 2, 71-89.

5. Fagerstrom, A., Ghinea, G. (2010) Web 2.0's Marketing impact on low-involvement consumers, Journal of Interactive Advertising, 10, 2, 67-71.

6. Bennett, J., Owens, M., Pitt, M., Tucker, M. (2009) Workplace impact of social networking, Property Management, 28, 3, 138-148.

7. Kaplan, A., Haenlein, M. (2010) Users of the world unite: The challenges and opportunities of social media, Business Horizons, 53, 59-68.

8. Vayrynen, K., Hekkala, R., Liias, T. (2013) Knowledge protection challenges of social media encountered by organizations, Journal of Organizational Computing and Electronic Commerce, 23, 34-55.

9. Clark, L., Roberts, S. (2010) Employee's use of social networking sites: A socially irresponsible practice, Journal of Business Ethics, 95, 507-525.

10. Delaney, A. (2011) Social networking – what about privacy and expression? Employment Law Bulletin, 4, 6-7.

11. Taylor M., Haggerty, J., Gresty, D. (2010) The legal aspects of computer usage policies Computer Law and Security Review, 26, 1, 72-76.

12. Morrison, T. (2014) Private eye: Legal update data privacy, The New Law Journal, 164, 7599, 164 NLJ 14

13. Piscotty, R., Voepel-Lewis, T., Lee, S., Annis-Emeot, A., Lee, E., Kalisch, B. (2013) To tweet or not to tweet? Nurses social media and patient care, Nursing Management, 44, 5, 52-53.

14. Lesnykh, A. (2011) Data loss prevention: a matter of discipline, Network Security, 3, 18-19.

15. Sipior, J., Ward, B., Volonino, L., MacGabhann, L. (2013) A framework for the e-discovery of social media content in the United States, Information Systems Management, 30, 14, 352-358.

16. Hutchings, G. (2012) Commercial use of Facebook and Twitter – risks and rewards, Computer Fraud and Security, 2012, 6, 19-20.

17. Moore, K. (2014) Social media 'at least half' of calls passed to front-line police, BBC News 24th June 2014, http://www.bbc.co.uk/news/UK-27949674

18. Mohd Zainudin, M., Merabti, M., Llewellyn-Jones, D. (2011) Online social networks as supporting evidence: A digital forensic investigation model and its application design, in Proceedings of IEEE International Conference on Research and Innovation in Information Systems, 23-24 November 2011, Kuala Lumpur, Malaysia, pp 1-6

19. Angelopoulou, O., Vidalis, S. (2013) Towards 'crime specific' digital investigation frameworks, in Proceedings of 3rd International conference on Cybercrime, Security and Digital Forensics, 8-9 June, 2013, University of Cardiff, Cardiff, Wales, UK, http://eprints.staffs.ac.uk/1314/

20. 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

21. Taylor M., Haggerty, J., Gresty, D. (2007) The legal aspects of corporate computer forensic investigations, Computer Law and Security Review, 23, 6, 562-566.

22. O'Floinn, M., Ormerod, D. (2011) Social networking sites, RIPA and criminal investigations, Criminal Law Review, 10, 766-792.

23. Gogolin, G. (2010) The digital crime tsunami, Digital Investigation, 7, 1, 3-8.

24. Haggerty, J., Casson, M., Haggerty, S., Taylor, M. (2012) A Framework for the forensic analysis of user interaction with social media, International Journal of Digital Crime and Forensics, 4, 4, 15-30.

25. Bader, M., Baggili, I. (2010) iPhone 3GS forensics: Logical analysis using Apple iTunes Backup Utility, Small Scale Digital Device Forensics Journal, 4, 1, 1- 15.

26. Morrissey, S. (2010) iOS Forensic Analysis: For iPhone, iPad and iPod Touch, Apress, New York, NY, USA, p 185.

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

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

29. Smith v ADVFN Plc & Ors, Court of Appeal - Queen's Bench Division, July 25, 2008, [2008] EWHC 1797 (QB)

30. Bond, R. (2010) Data ownership in social networks – a very personal thing, Privacy and Data Protection, 11, 1, 8.

31. Van Alsenoy, B., Ballet, J., Kuczerawy, A., Dumortier, J. (2009) Social networks and web 2.0: are users also bound by data protection regulations?, Identity in the Information Society, 2, 1, 65-79.

32. Marsoof, A. (2011) Online social networking and the right to privacy: The conflicting rights of privacy and expression, International Journal of Law and Information Technology, 19, 2, 110-132.

33. Muir, A. (2013) Online copyright enforcement by Internet service providers, Journal of Information Science, 39, 2, 256-269.

34. Griffin, J. (2010) The effect of the Digital Economy Act 2010 upon semiotic democracy, International Review of Law, Computers and Technology, 24, 3, 251-262.

35. Spaulding, T. (2010) How can virtual communities create value for business? Electronic Commerce Research and Applications, 9, 38-49.

36. Lane, S. (2011) English libel law is not fit for purpose, Serials, 24, 2, 150-153.

37. Lieber, L. (2011) Social media in the workplace – proactive protections for employers, Employment Relations Today, 38, 3, 93-101.

38. Nosko, A., Wood, E., Molema, S. (2010) All about me: disclosure in online social networking profiles: The case of Facebook, Computers in Human Behaviour, 26, 3, 406-418.

39. Zakaria, S. (2013) The impact of identity theft on perceived security and trusting E-commerce, Journal of International Banking and Commerce, 18, 2, 1-11.

40. Haralambos, N., Geach, N. (2010) Why the legislative provisions governing harassment lack clarity and cohesion, Criminal Law and Justice Weekly, 174, JPN 409.

41. Church, E., Fafinski, S. (2011) Social networks, crime and the law, Student Law Review, Autumn 2011, 13-16.

42. Pritchett, S. (2011) How do employers protect data from theft by their employees? Privacy and Data Protection, 11, 5, 8-14.

43. Yan, G., Chen, G., Eidenbenz, S., Li, N. (2011) Malware propagation in online social networks: nature, dynamics, and defense implications, In Proceedings of 6th ACM Symposium on Information, Computer and Communications Security, March 22-24, 2011, Hong Kong, pp 196-206