

A complex network diagram with numerous nodes and connecting lines, rendered in shades of grey and blue, serves as the background for the slide. The nodes are represented by small black dots, and the lines are thin, dark grey or blue. The overall structure is a dense web of connections, with some nodes having more connections than others, suggesting a social or data network.

Forensic investigation of social networking application

Dr Mark Taylor, Dr John Haggerty, David Greety, Peter Almond, Dr Tom Berry

Digital Forensic

Seunghee Seo

2017-11-20

Table of Contents

1 Introduction

- ## **2**
- (1) Forensic procedure**
 - (2) Evidence acquisition**
 - (3) Copying a website**
 - (4) Retrieving digital evidence**
 - (5) Analysing acquired data**
 - (6) Reporting evidence**
 - (7) Legal aspects**
 - (8) Data protection**
 - (9) Regulation of Investigatory Powers Act**
 - (10) Copyright/Defamation/Identity theft/Harassment
/Confidential information/Malware**

3 Conclusions

1. Introduction

What is social network application?

- Social networking applications provide facilities including email, blogging, instant messaging and photo sharing for social and commercial exchange.
- An increasing number of organisations use social networking app as part of their marketing campaigns
- Facebook, LinkedIn, MySpace, Twitter



Twitter post

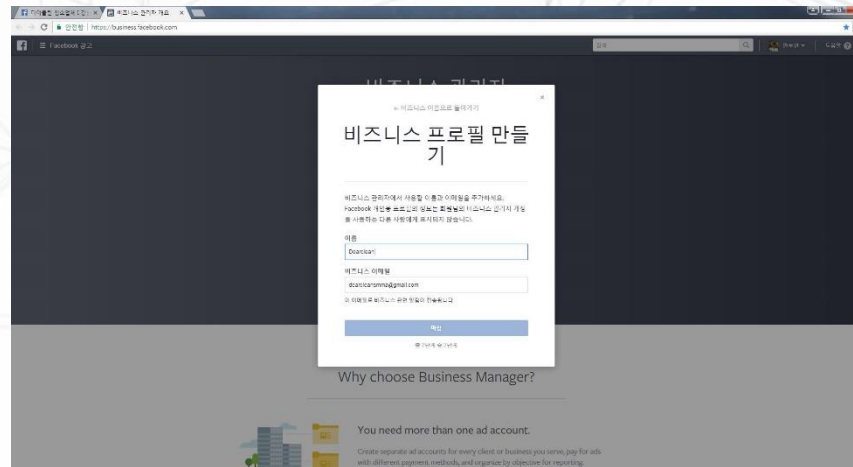


Facebook post

1. Introduction

1. Social networking as marketing campaign.

- 1) Some organisations actively encourage their employees to use social network application within the work environment to improve productivity via enhanced information sharing above and beyond the corporate network.
- 2) However, some organisations might not fully appreciate the potential for misuse that social networking applications may provide.
- 3) If organisations do allow employees to use social networking applications within the work environment, it would be prudent to set out guidelines for such in the organization's computer usage policy



Facebook business account

1. Introduction

2. Misuse of social networking application

- 1) Misuse of social media may occur in many different forms
- 2) Defamation of individuals
- 3) To nurses violating patient rights through misuse of social media
- 4) Data loss occurring to organisations

3. Purpose of forensic investigation of social media

- 1) To gather evidence evidence for use in a criminal trial
- 2) To use in corporate disciplinary panels for employees

2-(1) Forensic Procedure

1. Request for forensic investigation

- 1) An individual employee or police officer report suspected misuse to the relevant authority (manager in an organisation or local police force)
- 2) Or a request might be made to the provider of the social networking application for the relevant digital data relating to suspected misuse.

2. Request for forensic investigation

- 1) Digital evidence might be obtained from the web pages of the social networking application containing the material associated with the suspected misuse. (except private pages)
- 2) A next step might be to obtain digital evidence from the individual's computer
- 3) It may be necessary to examine a range of computing devices that may have been used by in misuse of the social networking application. (ex. Personal computer, laptop, tablet, telephones, digital assistants and games consoles)
- 4) The server computers supporting the social networking application might need to be forensically examined.

2-(2) Evidence Acquisition

1. Relevant social networking application web page

- 1) Significant changes may be made to a web page at any time from the message or post was initially made, to the time when the investigator attempts to make a copy of the page.
- 2) 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
 - The suspect's computing device : social media can be accessed across a variety of platforms from mobile phones
 - The victim's computing device : Although the victim's machine can be useful for the investigation, service provider logs potentially provide the best evidence.

2-(2) Evidence Acquisition

2. Social networking service's server computers and internet service provider's server computer

- 1) It would only be available for police investigations
- 2) The most convenient method of recovering the evidence may be to visit the website and take copies of the relevant content.
- 3) 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.

3. log

- 1) 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.

2-(3) Copying a website

- 1) To visit the website and record the relevant web pages using video capture software
- 2) Capturing the web pages using website copying software
- 3) Copying the web pages (saving code from the web pages)
- 4) For police investigations where there is difficulty in capturing the evidence, It might be possible to make an official request to the owner of the website.
- 5) Making a request to the service provider hosting the website. (log about access IP)
- 6) Making a request to ISP(internet service provider) logs of the times and dates and the identity of user allocated any IP address.
- 7) It may be possible to recover evidence of the website contents from and end user device

2-(4) Retrieving digital evidence

- Access to 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.
- If an individual sent the post from their private devices, the organization would not have the authority to access this devices.
- Existing computer forensic tools are designed to analyse evidence retrieved from storage media rather than examine data from online sources such as social media.

2-(4) Retrieving digital evidence

1. Finding social media artefacts on a computing device

- 1) Determining which social networking software, operating system, Internet browser.
- 2) Facebook artefacts could be located in the browser cache, unallocated clusters or system restore points of a computer.

2. Finding social media artefacts on mobile device

- 1) Examining data from mobile telephones and tablets can be somewhat more complex due to the variety of proprietary operating systems in use on such devices.
- 2) The different social media applications may store digital data in different formats and locations in the memory of the device.
- 3) Digital evidence relating to social media usage could be acquired by either a physical and logical

2-(5)Analysing acquired data

- Using an appropriate search approach can reduce the time and effort required to find either particular communication data or establish a particular pattern.
 - The specific individuals or groups with which the suspect has communicated via social media.
 - Specific timeframes within which social media communication took place.
 - The pattern of communication via social media
 - The artefacts relating to possibly more social networking applications.
 - The types of media used in the communications.

2-(6) Reporting evidence

- 1) A report would typically be produced detailing the relevant evidence found and the process by which the evidence was obtained.
- 2) When presented, evidence may be highly influential with jurors because it is a familiar medium, and it will often represent the very words typed or the images uploaded by defendants.
- 3) Printouts of social media communications are considered documents.
- 4) Authentication issues relating to digital evidence from social media may relate to accuracy of the exhibit, proof of authorship, identification of individuals in photographic evidence, and unfairly obtained evidence.

2-(7) Legal aspects

- 1) Any forensic investigation of misuse of social networking applications should follow the UK ACPO guidelines.
- 2) The Crown Prosecution Service guidelines on prosecuting cases provide guidance concerning the offences that are likely to be most commonly committed by the sending of communications via social media.

2-(8) Data protection

- 1) Personal data obtained during a computer forensic investigation of social networking applications misuse should not be accessible to those outside the investigating team.
- 2) The potential danger with social networking applications is that employees may view personal data in a different manner on social networking applications.

2-(9) 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 organisation or the relevant Internet service provider might be subject to the provisions of the UK Regulation of Investigatory Powers Act 2000

2-(10) Criminal activity in social networking application

1. Copyright

- 1) Social networking applications allow users to upload digital content that can be accessible to other users.
- 2) Such digital content uploaded by user might be copyrighted materials.
- 3) Organisations such as the Federation Against Copyright Theft may contact organisations where employees may have infringed copyright via social networking applications

2. Defamation

- 1) An employee (or organisation) 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 organisation via a social networking application

2-(10) Criminal activity in social networking application

3. 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
- The criminals use the identity of an individual through information through a social networking application of illegal activities.

4. Harassment

- Employees can upload materials via a social networking application that could constitute harassment of another employee, customer or client of the organisation
- Employees 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

2-(10) Criminal activity in social networking application

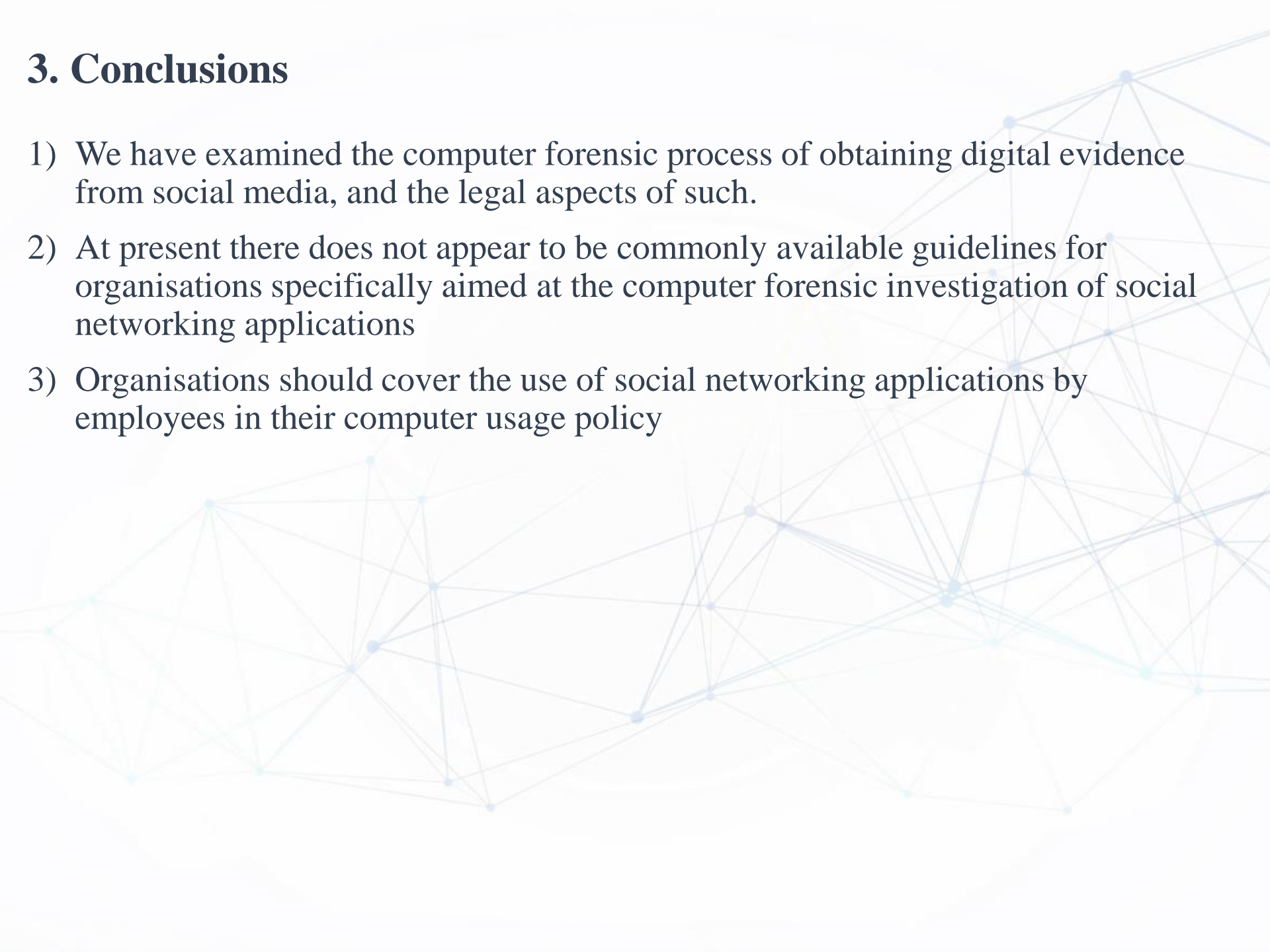
5. Confidential information

- Employee may inadvertently disseminate confidential information relating to an organisation via a social networking application.
- information relating to the financial state of the organisation, contracts, projects or products or services or other confidential information
- Ex. LinkedIn

6. Malware

- The widespread use of social media provides a platform for the spread of malware such as computer viruses, worms, trojans 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

3. Conclusions

- 1) We have examined the computer forensic process of obtaining digital evidence from social media, and the legal aspects of such.
 - 2) At present there does not appear to be commonly available guidelines for organisations specifically aimed at the computer forensic investigation of social networking applications
 - 3) Organisations should cover the use of social networking applications by employees in their computer usage policy
- 



Q&A