Legal Issues for Computer Forensics

Angela Brungs - Researcher
Rodger Jamieson - Director

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
e-mail: r.jamieson@unsw.edu.au

Abstract

The adoption of computers into every aspect of modern society has been accompanied by the rise of e-crime. The processes and techniques employed by the field of computer forensics offer huge potential for the extraction and presentation of electronic evidence in a court of law. Yet, the current research that has been conducted in this field is minimal. In this study, current and potential IS legal issues that impact on the computer forensic field are analysed. Due to the field being comprised with aspects of both law and computers this causes much conflict, mainly due to the law's inability to adapt and evolve as quickly as the computing environment.

Keywords

Electronic Commerce, Computer Crime, E-crime, Computer Forensics, Electronic Evidence, Digital Evidence

INTRODUCTION

The computer has become a necessity to modern society. The amalgamation of the communication and the computing field has permitted computers worldwide to be linked together in large networks. However, the growth of this electronic environment has not come without a corresponding growth in electronic crime. To prosecute electronic offenders, new forensic process and techniques were developed to retrieve evidence off computers, and new laws had to be proposed to govern the admission of such evidence. These processes and procedures are now collected into the field of computer forensics (McKemmish, 1999). This new field must deal with the demands of the evolving computer world, as well as emerging legal processes, rules of evidence and court procedures that particular jurisdictions impose on the collection, analysis and presentation of the evidence.

The aim of this research study is to identify and examine the key legal issues driving the development of the computer forensic field. The treatment of electronic evidence in court is still a new area with regards to admissibility of computer produced evidence. Since the prime purpose of computer forensics is the production of evidence that can be accepted by a court of law, the legal environment has a great influence on the methods that computer forensic specialists employ. There has, however, been limited research conducted into the methods of computer forensics (Tennyenhuis & Jamieson, 2003), with most of the research carried out, held as confidential information within the domain it was created, for example law enforcement.

Therefore, a fundamental step to further develop the field, is to use exploratory research techniques to identify and highlight existing and potential legal issues. The scope of this research, rather than to provide solutions, is focussed on identifying issues. It is the first paper in a wider study which aims to develop a categorisation of all the fundamental aspects of each issue, and propose a model that shows the inter-relationships that exist between each issue. This will allow the key issues in the computer forensic area to be distinguished for future research. If these issues are not resolved they could potentially present a major problem in the future, and may severely limit the field's advancement.

E-CRIMES

It is difficult to overestimate the impact of the electronic world on contemporary Western society. In 2001 there were 574 million people throughout the world who were connected to the Internet with projections indicating a further increase to 741 million during 2002 (Intergov International, 2002). While beneficial in many ways, access to this new technology has come with a price. The rapid uptake of technology has been accompanied by a significant growth in computer crime (Interpol, 2002). The impact on business has been significant with average US losses reported of $4.6m from financial fraud and 80% of respondents experiencing financial losses through computer security breaches (CSI/FBI 2002).

Few state bodies articulate a clear definition of computer crime (or e-crime). The best definition of e-crime, which comes from DIBS technology consulting group (2002), is:

- "a criminal act in which a computer is essential to the perpetration of the crime, or
- a criminal act where a computer, non-essential to the perpetration of the crime, acts as a store of information concerning the crime."

E-crimes are essentially crimes where the computer is used either as a tool to commit the crime, as a storage device or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime or information that is illegal for the owner to possess, such as stolen intellectual property (Australasian Center for Policing Research - ACPR, 2000). Computers are classified as a target if the information that they contain is altered or retrieved in any unlawful way. Such crimes can range from amateur hacking to terrorism.

RESEARCH METHODOLOGY

A computer forensics research forum was held which involved a group discussion focussed on determining the foremost legal issues for experts working in the computer forensics field.

The experts were asked to identify what they believed were key issues and problems facing the development of the field. Using the Delphi technique, issues were first raised during a discussion and brainstorming session. In the remaining time, a two-fold approach was used to determine which issues were regarded as the most important to be resolved. This rating technique was deemed more suitable than judging the importance of the issue by how many people supported it in the general conversation so as not to neglect quieter members. It is therefore not possible to relate the number of participants raising each issue. With the Delphi technique, the participants firstly allocated the issues with an importance level. This was achieved using a 7-point Likert scale. A Likert scale is a way to measure a respondent's degree of agreement or disagreement with a particular item (Judd et al., 1991). Each item was allocated a scale from 1, which was classed as unimportant, to 7, which was classed as very important. The participants were also asked to rank all the issues in order from one to seventeen, where number one would have the top priority for resolution. Experts were asked to allocate these rankings on the basis of what was important for their current work. This two-fold approach was used because a simple importance rating may not have adequately differentiated the issues. To capture the discussion, two tape recorders and a mini-disc were placed evenly around the room.

The forum brought together participants from several different core functional areas:

- law enforcement;
- government regulators;
- consulting companies; and
- academics.

Preliminary interviews were used to identify key personnel from these sectors with knowledge specific and relevant to the computer forensics area. These candidates were all highly regarded by their peers for their knowledge, experience and the roles they hold within the area of computer forensics.

The Law Enforcement participants consisted of members of the Australian Federal Police (AFP), the NSW Police Force and the Victorian Police Force. Government regulators included representatives from the Australian Securities and Investment Commission (ASIC), National Crime Authority (NCA) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). These two groups are both commissioned by the government and work closely together on computer forensics issues. The third group comprised of employees from consulting companies. These representatives manage the computer forensics or computer security sections of three major accounting/consulting firms. Two members of this group had previously worked for computer investigation units in the Australian State Police Forces. The last group, 'Academic', consisted of a representative whose area of research concerns computer crime.

Three of the above participants were not able to make it to the forum but still wished to participate in the research. They completed the Delphi coding form within three months of the forum. These participants were the representatives from Victorian Police Force, ASIC and NCA.

RESULTS AND DISCUSSION

The results obtained from the forum are shown below, firstly with an explanation of the identified issues, and then the evaluation of the ranking and ratings given to the issues.

The members of the forum listed 17 issues as pivotal problems in the computer forensics area needing further research. These issues and what they represent are listed below:

1. Jurisdictional – The issue of jurisdiction concerns the differences between state and federal legislation. Recent legislative amendments to the national computer crime laws, such as the NSW Crimes Amendment (Computer Offences) Act 2001, have caused uncertainty within the industry. However it was noted that while the differences in jurisdictions presented a problem, it was fundamentally due to the mechanics of the legal system, and was simply a problem that just had to be dealt with in the course of the work. The group did feel, however, that detailed research needed to be conducted in order to identify the pivotal issues related to jurisdictional differences.

2. Computer Evidence Presentation Difficulties - This issue is closely related to 'jurisdictional' (above). However, the main focus of 'computer evidence presentation difficulties' is the obstacles that the differences in jurisdictional laws create in a court. The legislation of the individual states and the Commonwealth differ with respect to the presentation and admissibility of computer evidence. This leads to a situation where the location of the court forms part of the consideration for evidence admissibility. The significance of this is that some forms of digital evidence can be accepted in some states, but not in others. There are also different requirements in each state for particular forms of digital evidence such as e-mail, video footage, Microsoft PowerPoint presentations and recorded evidence. Thus for presentation in court, experts must ensure that all such requirements are met. An expert who is required to present evidence across states will need to know all the variations and ensure that their evidence handling procedures have met all the criteria. It was noted that the NSW and the Commonwealth have a codified act whose electronic evidence-friendly nature simplifies the admissibility and presentation of such evidence. (Refer EFA 2003 for a summary of legislation relating to Cyber crime).

3. Requirements to 'Fire Up' Original - This issue primarily deals with the need for a best practice guide. One expert commented that in Queensland there is a practice to 'fire up' the original computer in court when presenting the electronic evidence. The problems that this requirement raises are numerous, including the implications for an appeal situation, as the computer is no longer in its original state, and the problems this would pose for large corporate systems. The crux of this example serves to highlight the need for a best practices guide for computer forensics. This methodology should cover the acquisition, preservation, analysis and presentation of the evidence. There is also a need for this methodology to be standardised nationally and internationally.

4. Computer Literacy in the Legal Sector - For electronic evidence to be satisfactorily accepted into the legal environment there has to be acceptance from those working within the sector. There is some concern that an impediment to the more widespread presentation of electronic evidence is the lack of understanding and comprehension by lawyers, judges and juries, of what the evidence signifies. A low standard of computer literacy in the legal sector could potentially have a large impact on the computer forensics area as unrealistic and incorrect demands and precedents are placed upon electronic evidence.

5. Confidential Records, Business Systems - Evidence collection forms a large component of computer forensics work. The issue raised refers to the problems that confidential records have on evidence collection. There seemed to be much uncertainty about the correct proceedings when dealing with these situations, and whether there are the required legislative mechanisms in place to manage them. For law enforcement, care must be taken that any evidence gathered does not infringe on professional privilege rights.

6. Telecommunications Act Covering Data - This issue is focussed on the potential implications that the Telecommunications Act has on data interception. A point was raised in the forum that while the Telecommunications Interceptions Act covers only the interception of traffic over the telecommunications system and the data for communications, there is uncertainty as to when this act can be applied. For, while data may not yet have been accessed, it may have been stored electronically whilst in transit. Thus, while the Telecommunications Interceptions Act does not directly cover stored data, there are situations where this act could be applied. The uncertainties concerning the coverage of the Telecommunication Interceptions Act needs to be resolved.

7. Criminal Prosecution vs Civil Trial - Participants in the forum felt that research needed to be conducted to investigate the differences between a criminal prosecution and a civil trial and the impact that those differences have. The aim of this is to ascertain the best instances for a civil trial. This would allow the progression of the computer forensics field away from police and government regulators base. In many situations, companies are not looking to prosecute an offender, but rather wish to stop the incident and prevent the occurrence from happening again. The most obvious difference between a criminal and civil investigation is the investigatory power of the investigators. For example, currently much of the information to support an investigation is gained by the police using specific powers such as search warrants and the Telecommunications Interceptions Act.

However, consulting companies conducting private investigations are not able to obtain a search warrant and must therefore find other instrumental means, such as an Anton Pillar order, to legally obtain the data.

8. Privacy Issues / Workplace Surveillance - The introduction of privacy legislation has created uncertainty in computer forensics with regard to what is permissible behaviour in collecting and retrieving personal information. These privacy provisions have not been adequately tested in the courts to provide a comprehensive common law background. This issue is of primary concern to private consulting companies working in the area. Uncertainties mentioned include: 'What is legal for companies to do?', 'What is a breach of an employee's privacy?', and 'What data can be safely taken from a computer?'.

9. Interpretation of Telecommunications Act - While similar to the 'Telecommunications Act Covering Data' issue, this issue is specifically focused on the uncertainty of the exact particulars of when a communication has taken place, especially in relation to e-mails. The questions raised in this issue include: 'When is an e-mail classified as read or unread?', 'What point marks the beginning and the end of a communication?', 'Where does a network start and finish?', and 'Is imaging an unread e-mail contravening the Telecommunications Act?'. The participants felt that resolving these interpretations for e-mails was quite important, as it would have an impact on all other forms of communication content.

10. Access and Exchange of Information - This is another issue relating to privacy, in particular how to preserve the privacy of clients, while also gaining enough information to successfully complete an investigation. There still exists uncertainty for some providers of information, such as the telecommunications companies and ISPs, as to when they can gather and provide information to the police, and how to protect the privacy and confidentiality of their clients. It was also noted from the experienced practitioners that many offences might be ignored as private companies refuse to report the crime to the police fearing the negative publicity from a public announcement. The principles of access and exchange of information need to be worked out so that a smoother process can be ensured.

11. International Cooperation in Practice - International cooperation is essential for computer forensic work as gathering digital evidence may require national borders to be traversed. For example, information may need to be accessed from a server in a different country. There is currently considerable discussion in the industry about international cooperation. However, research needs to be conducted to determine the requirements to make international cooperation work in practice. Research would include investigation of the compatibility of legal systems, and whether the current policy makers appreciate these differences and the need for international cooperation when proposing new legislation. It also would include outlining the problems concerning the conflict between common law and civil law jurisdictions.

12. Revision of Mutual Assistance - While focussing on an area similar to the previous issue 'International Cooperation In Practice', this issue relates to the current regime for exchange of information between countries. The experts feel that there are currently many problems associated with this scheme, such as inability to work in real time and are unsure of its ability to stand up to the pressures that the digital environment has placed upon it. This suggests a revision of the Mutual Assistance scheme is required to ensure that proper processes are still used, but allow information to be accessed in real time.

13. Contrast of Broadcast Vs Communications - This issue addresses the particulars of the definitions of Broadcast and Communications Acts, and thus how they are treated under the relevant legislation. Currently communications is legislated under the Telecommunications Act, while Broadcast has been included in the Commonwealth Copyright Amendment (Digital Agenda) Act 2000. Once again, the lack of cases dealing with this issue in Australian law courts has prevented clarification of some of the finer points.

14. Do We Need New Offences? - Recently new offences have been enacted into Australian legislation, through amendments to the Crimes Act (Cth 1914), to deal with electronic and digital communications. This issue focuses on the need to examine the adequacy of these offences. These new offences include unauthorised impairment of data or electronic communication, and possession or supply of data with intent to commit a serious computer offence.

15. Launching Actions Against Persons Unknown in a Civil Trial - This issue highlights the difficulty for the private sector obtaining access to information. For a civil litigation, in order to subpoena information such as the offender's identity from communication companies, a civil case must first be launched. However, to launch a civil action a person must be named and cases cannot be launched again persons unknown. This is a major obstacle in evidence collection for non-government organisations and remedies need to be developed.

16. Technical Issues – Testing of Tools and Techniques - To analyse, collect, preserve and present evidence, forensic experts use a variety of tools and techniques. This issue deals with the need to ensure that third party validation of tools and techniques are conducted. This is to ensure that a scientific methodology is applied within the field to guarantee repeatability and verification of techniques and findings. Without this, the courts

cannot be assured of the reliability of a tool or technique other than by the fact that it might have been used in previous cases, a method which does not always ensure that the best practices are embraced.

17. Court Reporting Skills and Techniques – Expert Witness - Practitioners believe that guidelines outlining the minimum requirements for the skills and qualification levels to attain 'expert' status in the courts needs to be defined. This could incorporate required skill sets, minimum working experience, and formal qualifications such as a university degree or commercial certification.

RATING AND RANKING OF ISSUES

Every issue was given an importance level and a ranking by each expert participating in the forum. Due to limited time, there were not multiple ranking rounds to ensure that the panel reaches a level of consensus of the importance of each issue. While this could impact on the results, the data obtained provide valuable information on the experts attitudes to the issues. The results in Figure 1 below shows the data complied from the forum. The ranking and the importance level columns represent the average value of the participant's responses.

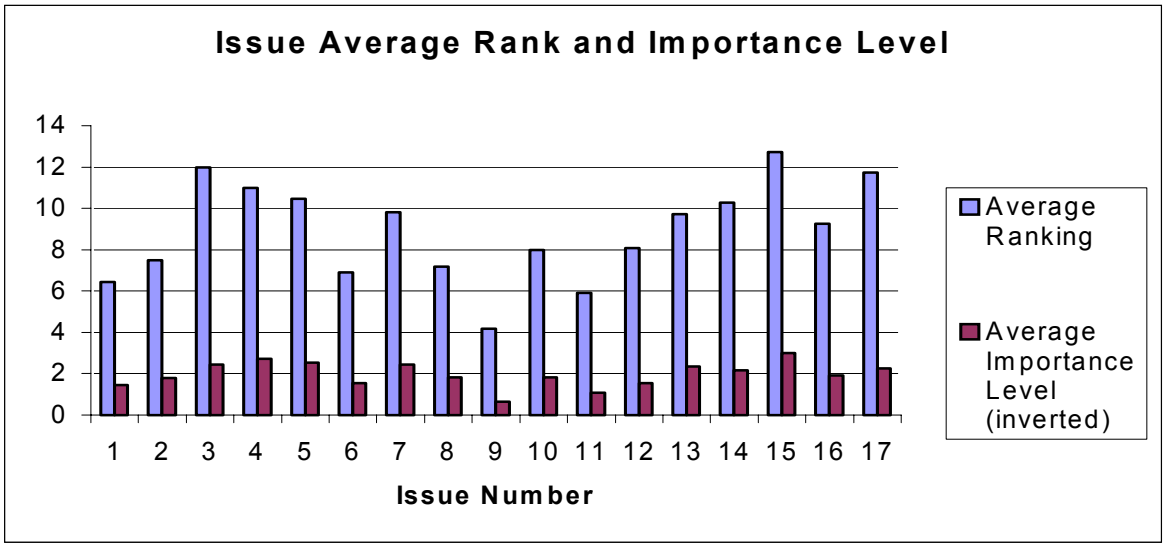

Figure 1: Average Rank and Inverted Average Importance Level of Each Issue.

As can be seen in the Figure 1 above, all issues identified have an average inverted importance rating of less than 3, which was the medium point in the adopted Likert scale. This shows that all issues raised were considered at least in the range of important to very important. This result was not unexpected, as the task given to the experts was to raise any issues that they felt were important to computer forensics. Therefore only issues that they classed as important were raised, which is reflected in the results. However, there could have been a situation where an issue was raised that, whilst important to one expert in their line of work, did not relate to the overall field. The consensus on the level of importance of all the issues confirms that this did not occur, and that all the issues raised are important to all functions within the field.

Figure 1 also shows what seems to be a relationship between the average importance rating and the average rank assigned to the issues. This indicates that there is a consistency between the two evaluation techniques used.

	Frequency			
Issue Number	**1-4**	**5 – 9**	**10 – 14**	**15 -17**
1	4	5	0	2
2	3	3	3	1
3	0	3	5	3
4	2	0	8	1
5	1	2	7	1
6	4	4	1	2
7	3	2	2	4
8	4	4	2	1
9	6	4	1	0
10	2	6	2	1
11	7	2	2	0

12	2	5	3	1
13	3	1	4	3
14	0	4	5	2
15	1	1	5	4
16	2	5	2	2
17	1	3	3	4

Table 1: Ranking Frequency.

The high average values of the ranking's as shown in Figure 1 reaffirm that priority ranking's varied across the panel. Table 1 is a frequency table of the issue ranking's. For example with issue 1, four experts gave the issue a ranking within the top four, five ranked the issue between five and nine. In Table 1 it may be seen that the majority of the issues were given a ranking within each of the frequency sets. In addition, the experts opinions were divided for every issue with no one issue being seen by all as important or non-important. In particular, 'Court Reporting Skills', 'Contrast Of Broadcast Vs Communications' and 'Telecommunications Act Covering Data' all had at least one expert consider the issue the most important, and another expert considered the issue as the least important, ranking it number seventeen. As the importance of an individual issue largely depends on the task that a computer forensic expert performs in their work environment, this variance is expected.

Figures 2 and 3 show the average ranking's when split into the functional areas of 'Law Enforcement', 'Government Regulators' and 'Consultants'. The results collected for the role of the 'Academic' is not displayed as with only one participant, the sample population is not large enough to draw generalised conclusions.

Participants from the private sector considered 'Privacy Issues' as the key issue for computer forensics. However this was only given an average ranking of ninth by the police and government regulators. In the course of their work, private consultants have to protect the privacy of their clients and employees in order to safeguard themselves from future litigation. However, when police are investigating a criminal matter, no consideration is taken to ensure that certain information is kept private if it has relevance to the case.

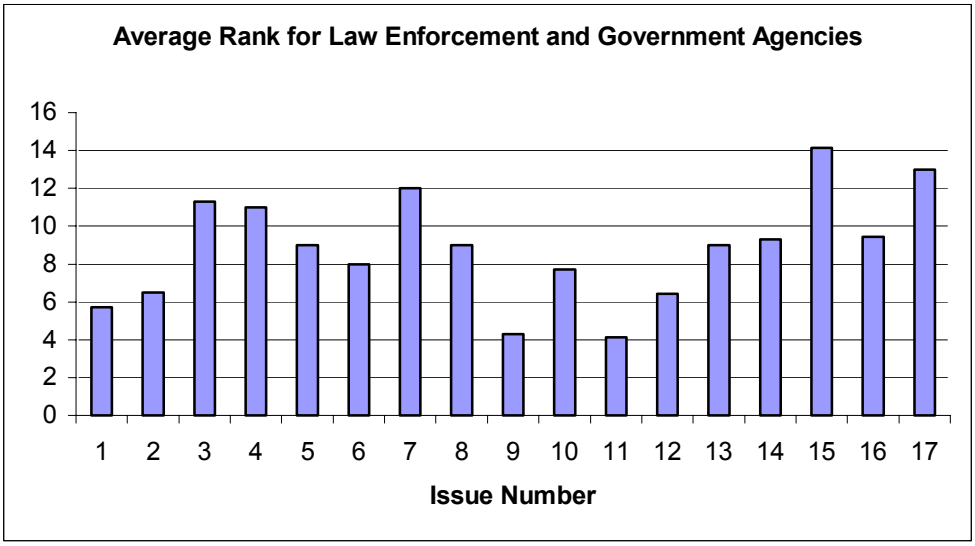

Figure 2. Average Rank for Law Enforcement and Government Agencies.

On the other hand, the police and government regulators placed 'International Cooperation In Practice' as their number one issue, while the private consultants ranked it in tenth place. Members of the federal police, AUSTRAC and ASIC in particular, constantly deal with information exchange across international borders and facilitation of this is of primary concern. The issue 'Revision Of Mutual Assistance', which is also related to information exchange between countries, was given an importance rating of 6.14 by the police, rating as one of their top three issues. Yet the importance level that the private consultants gave 'Revision Of Mutual Assistance' placed it as the issue with the lowest importance level.

Nevertheless there was some agreement between the police and government regulators and the private consulting companies on particular issues. Both groups assigned the issue, 'Interpretation Of The Telecommunications Act', a ranking of number 2, and 'Do We Need New Offences' a very low ranking.

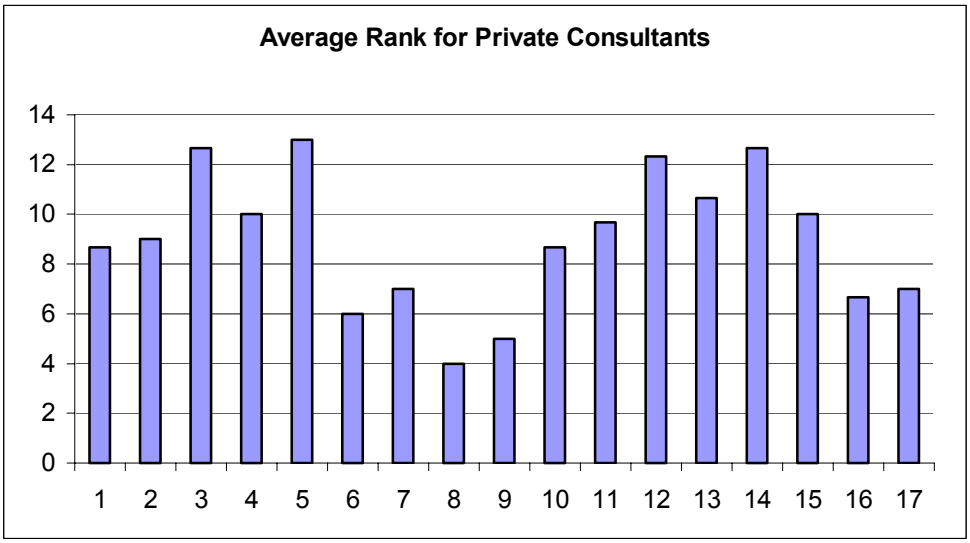

Figure 3. Average Rank for Private Consultants.

Due to the discrepancies between the core areas of computer forensics, the below Figure 4 shows the ranking and the importance level columns using an average-weighted value of participants' responses. Weighted values were used to prevent particular functional areas from biasing the results. This technique was adopted due to the prominence of the police and government regulators within the sample. Thus the results were divided up into three core functionality group, 'Police and government regulators', 'Consulting companies and 'Academics' and weighted to give each group equal significance.

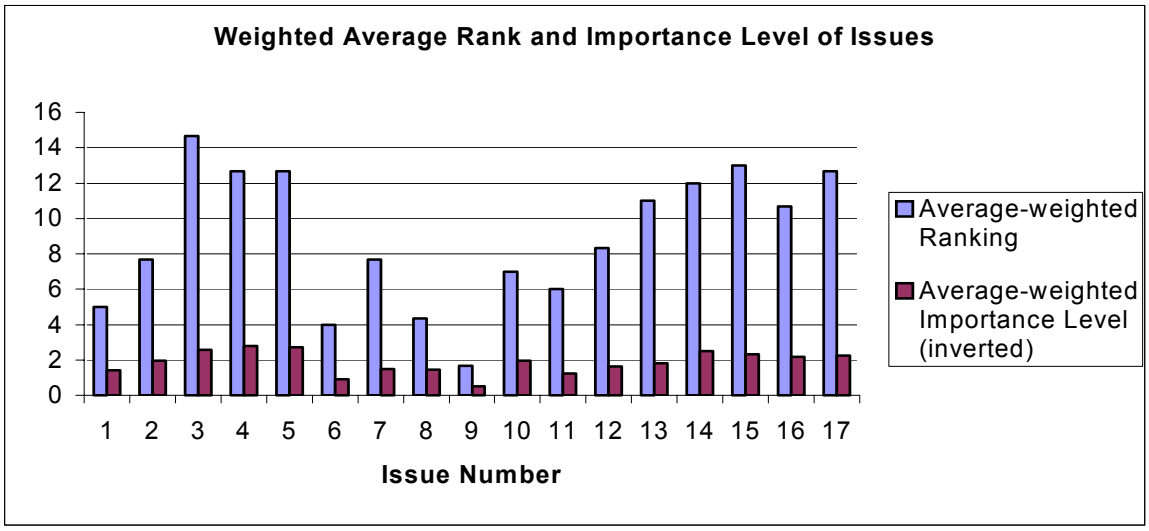

Figure 4: Weighted Average Rank and Importance Level of Issues.

In Figure 4, issues classed as most important to all experts in the group were 'Interpretation Of The Telecommunications Act', 'Privacy Issues', 'Jurisdiction' and 'Telecommunication Act Covering Data'. These results indicate that there is a lot of uncertainty about the interpretation of new legislation and it is a fundamental cause of concern within the industry. The issues classed as least important were 'Requirement To Fire-up Original', 'Computer Literacy in the Legal Sector' and 'Launching Actions Against Persons Unknown In A Civil Trial'.

CONCLUSION

Modern society is characterised by an ever-increasing use of computer technology. Computers from all over the world can now be networked together via a digital environment that transcends jurisdictional boundaries. This increase in computer use has been accompanied by a rise in e-crime. To combat e-crime, processes and techniques have been developed to allow evidence to be extracted from digital devices. These processes and techniques are what comprise the field of computer forensics.

Of the issues identified above, three main areas are highlighted as key issues by experts during the ranking assignment in the forum. These three key issues are:

1. Judicial Flexibility;
2. Privacy; and
3. Multi-jurisdictional Nature.

'Judicial Flexibility' refers to the ability of legal systems to adjust to technological change. This issue is of paramount importance as without this, there will be no link between the technology and the judicial requirements. The legal issues of computer forensics arise out of incompatibility problems between the areas of computers and law. The requirements of 'Judicial Flexibility' include education for lawyers on technological issues as well as legal education for forensic specialists. Education reduces uncertainty between the legal and technical fields and improves the acuity of the resulting precedence. Legally, precedence is highly desirable to establish clear guidelines for computer investigation. Precedence helps to define boundaries in legislation as part of an on-going legal evolution process. Precedence evolution may be accelerated by thorough challenging of evidence presented to court. However, continuing efforts by both legal and computer fields towards better cohesion is essential.

'Privacy' is seen by many as a necessary right with regard to electronic data storage. Currently many are unaware of the extensiveness of data surveillance and the present transparency of the web. As this realisation increases, the demand for privacy will impact on computer forensics. Therefore the implications of privacy to computer forensic are yet to be fully realised. With this realisation further technologies and protocols will need to be adopted to preserve forensic incisiveness in the face of privacy restrictions.

'Multi-Jurisdictional Nature' is due to the cross-boundary environment of computer forensic investigations. Challenges arise both in obtaining evidence and in the prosecution of offences due to legal incompatibilities. These include differences in investigatory powers, offence definitions and the requirement for inter-government or inter-organisation cooperation. Concerted international cooperation is necessary for successful e-crime prosecutions across jurisdictions. This may be facilitated by the adoption of international treaties and revision of mutual assistance schemes.

This research study aimed to provide a better understanding of what legal issues affect computer forensics. The purpose of this research was to identify and categorise the key aspects of each issue, rather than provide solutions to the issues raised. The issues identified in the forum, and the current literature will be used in future research to classify the major issues into a taxonomy. This taxonomy will also include investigation into the relationships between the issues and this will provide a platform on which further research in the computer forensic area may be conducted.

REFERENCES

Australasian Centre for Policing Research (ACPR) (2000) The Virtual Horizon: Meeting the law enforcement challenges – Developing an Australasian law enforcement strategy for dealing with electronic crime, ACPR, Adelaide.

CSI/FBI (2002) 2002 Computer Crime and Security Survey, Computer Security Issues and Trends, 3(1), Spring, 1-22.

DIBS (2002) Computer Forensics, www.computer-forensics.com/investigation/welcome.html, Last visited 6th June 2002.

EFA (2003) Electronic Frontiers of Australia, Security Computer Crime pages http://www.efa.org.au/Issues/Security/ (last accessed 28 Aug 2003).

Intergov (2002) Intergov International Latest web statistics, http://www.intergov.org/public_information/general_information/latest_web_stats.html, Last visited on the 17th March 2002.

Interpol (2002) Interpol's contribution to combating Information Technology Crime, http://www.interpol.int/Public/TechnologyCrime/default.asp, Last visited 1st April 2002.

NSW Crimes Amendment (Computer Offences) Act 2001, NSW Parliament.

Judd M., Smith E., Kidder L. (1991) Research Methods in Social Relations, Harcourt Brace, Sydney.

McKemmish, R. (1999) "What is forensic Computing", Australian Institute of Criminology, Trends and Issues No 118, June.

Tennyenhuis, A. & Jamieson, R. (2003) An Investigation into Computer Forensics Methodologies and Competencies: A Research Report, Research Report No 1, SAFE Research Program, SIRCA, May.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the assistance and cooperation of participants at the SEAR E-Crime and e-Forensics Research Forum, held at the University of NSW in September 2001, in identifying key research issues in the e-forensics area.

COPYRIGHT