J Comput Virol (2011) 7:189–199
DOI 10.1007/s11416-010-0147-z

ORIGINAL PAPER

Managing university internet access: balancing the need for security, privacy and digital evidence

Vlasti Broucek · Paul Turner · Mark Zimmerli

Received: 16 July 2010 / Accepted: 23 October 2010 / Published online: 25 November 2010

Abstract The provision of high speed, reliable Internet access and the ability to support secure and flexible on-line systems for research, teaching and administration has become critical to the success of Australian Universities. An exponential growth in Internet traffic has led to ever increasing costs for the provision of these services at a time when most Australian Universities have been experiencing tighter budgetary conditions. Significantly, alongside these financial concerns, Universities have started to recognise the emergence of a range of other issues related directly to the nature of on-line behaviours engaged in by the diversity of users that Universities are now expected to support. These on-line behaviours are challenging Universities to find responses to balancing users' right to privacy and freedom of speech with the need to protect against legal action arising from criminal, illegal or inappropriate behaviours by some users on University networks. As part of the responses being developed, many Universities have introduced Internet Management Systems (IMS), similar to the systems used by many Internet Services Providers (ISPs). This paper presents a case study on the experience of the University of Tasmania (UTAS) in introducing an IMS. The case study covers the period from the initial 'call for proposals' through to the deployment of the new IMS system. The paper highlights that decisions pertaining to the IMS systems have direct implications for balancing the competing rights, interests and requirements of different stakeholders. More specifically the case study highlights the impact of the changing nature of users' relationships with the Internet and the need for vigilance on the part of users, network administrators, service providers and policy makers. The dangers of failing to get the right balance are presented and the paper argues for the importance of user education, change management and communication throughout the University and its broader community of users. The paper also briefly considers how Australia's planned accession to the Council of Europe's Convention on Cybercrime may impact on these issues. More broadly, this paper suggests that additional changes will emerge as IPV6, companies like Google and cloud computing architectures reconfigure individual users relationships with 'their' information and access to the Internet. These developments will continue to transform the meaning of concepts such as ownership and control, privacy and freedom of speech within and beyond on-line environments.

An earlier version of this case study was published in proceedings of the 19th Annual EICAR Conference 2010.

V. Broucek (✉)
School of Psychology, University of Tasmania,
Private Bag 30, Hobart, TAS 7001, Australia
e-mail: Vlasti.Broucek@utas.edu.au

P. Turner
School of Computing and Information Systems,
University of Tasmania, Private Bag 87,
Hobart, TAS 7001, Australia
e-mail: Paul.Turner@utas.edu.au

M. Zimmerli
IT Resources, University of Tasmania, Private Bag 69,
Hobart, TAS 7001, Australia
e-mail: Mark.Zimmerli@utas.edu.au

1 Introduction

Australian Universities are increasingly more dependent on being able to provide high speed, reliable Internet access and to support secure and flexible on-line systems for research, teaching and administration. Significantly, while most Universities continue to grapple with these issues, other challenges have emerged that relate directly to the nature of

on-line behaviours engaged in by the diversity of users that Universities are now expected to support. These on-line behaviours require Universities to find responses to balancing users' right to privacy and freedom of speech with the need to protect against legal action arising from criminal, illegal or inappropriate behaviours by some of these users on University networks. The University of Tasmania was directly involved in a case brought against it by Sony Music Entertainment (Australia) concerning copyright piracy on its networks [1–4]. This case has been extensively analysed [5–7]. As part of the responses being developed, many Universities have introduced Internet Management Systems (IMS), similar to the systems used by most Internet Services Providers (ISP).

This paper presents a short case study on the experience of the University of Tasmania (UTAS) in introducing an IMS. The case study covers the period from the initial 'call for proposals' through to the deployment of the new IMS system. The deployment of the full system has to-date been relatively restricted in the University and so the analysis presented is preliminary in nature. It is anticipated that a full survey of the entire University population will be conducted within the next 12 months.

The paper is divided in two parts:

Part one presents the case study covering the technical and organisational setting, the initial call and process of IMS selection, implementation and preliminary evaluation and includes a description of the IMS product. This part also briefly considers how Australia's planned accession to the Council of Europe's Convention on Cybercrime [8,9] may impact on the solution presented.

Part two discusses how decisions pertaining to IMS systems have direct implications for the balance of competing rights, interests and requirements from different stakeholders. The case study highlights the impact of the changing nature of users' relationships with the Internet and highlights the need for continued vigilance on the part of users, network administrators, service providers and policy makers. The discussion illustrates the dangers of failing to get the right balance and argues for the importance of user education, change management and communication throughout the University and its broader community of users.

2 Part one: University of Tasmania (UTAS) IMS case study

The University of Tasmania (UTAS) is a regional University with approximately 20,000 full time equivalent network users (15,000 students and 5,000 academic, administrative and support staff). The University teaches across three campuses in the Island State of Tasmania, as well as two campuses in Sydney and provides teaching services to several international campuses, including in Shanghai, China and Kuala Lumpur, Malaysia. All user Internet access is managed and provided through the Information Technology Resources (ITR) division of the University. As with other Universities around the world the University of Tasmania has become increasingly more dependent on being able to provide all its users with high speed Internet access and support for secure and flexible on-line systems for research, teaching and administration.

Rapidly expanding Internet usage over the 2000–2005 period had resulted in significant cost increases for the University in terms of bandwidth. Coupled with this was that the configuration of the proxy servers, and the protocols they monitored, meant that the University could not easily determine what, who, or how bandwidth was being consumed. The implications of the above situation were that the University was bearing increased Internet costs, without any way to investigate where the costs were being generated and whether management of the bandwidth, which relies on greater knowledge its use, could improve the Internet service for users and mitigate some of the costs for the University. Coupled with increased bandwidth usage was the emergence of several peer-to-peer networks which were difficult to monitor via proxy server information.The advent of peer-to-peer networks (e.g. BitTorrent and eDonkey) resulted in a major shift from http file sharing to the alternative protocols, and thus the University's proxy servers were neither controlling nor monitoring the vast majority of this traffic. The manner of these peer-to-peer networks made monitoring very difficult and connections appeared to use random ports and peers were members of a user swarm. No real picture of activity could be identified with the exiting information. Compounding the issues with peer-to-peer network access, media owners increased their enforcement activities between 2007–2010, necessitating improved monitoring and control of the University's Internet system to comply with the requirements of the media owners.

Until June 2010, University had in place an IT Facilities Usage Agreement, to which all staff and students were bound. This document dealt with issues of technology misuse, including copyright infringement. Following the approval of new ICT Security Framework in June 2010 (see Sect. 2.4 ICT Security Policy Framework for more details), this agreement was replaced by ICT Services and Facilities Use Policy. Information collected via the University's proxy servers made the enforcement of this agreement/policy difficult as investigation of cases of reported misuse were hard to conduct. An expansion of monitoring capacity was identified as necessary to identify misuse and control it.

Internet services are provided to UTAS by the Australian Academic and Research Network Pty Ltd (AARNet). For the purposes of billing, traffic sources are categorised into on-net domestic, on-net international, off-net domestic and off-net international. The University core data network infrastructure is built on CISCO hardware. The University

network is protected by a boundary firewall and multiple DMZ's are provided for with separate virtual firewalls. Currently UTAS employs four squid proxy servers requiring simple authentication. Internet HTTP and HTTPS services are only accessed via the proxy servers. FTP services can also be accessed via the proxy server but use of the proxies for FTP is not enforced. Log files from these proxies, and 'netflow' log files from AARNet, provide a very basic means of network traffic management and in the past were used in the determination of any inappropriate use. Software tools developed in house have also been used for generating Internet traffic reports.

By early 2007, the University had recognised that the continued almost exponential growth of Internet usage was quickly becoming unsustainable. As a result, senior management decided that UTAS must determine, in a more granular fashion, how the Internet was being used and by whom. After gathering this information and modelling the Internet usage, management anticipated that the University would be in a better position to be able to determine a strategy for managing its Internet traffic. At this time, the assumption was that the traffic management approach to be developed would be in one or more forms involving the application of quotas (soft or hard), back charging or traffic shaping.

In January 2008, UTAS ITR issued a RFP (request for proposal) seeking a supplier of a system to monitor Internet traffic at UTAS to commence in the first half of 2008 to determine by whom and how the Internet was being used. It was anticipated at the time that the monitoring system would provide traffic totals broken down by traffic source as defined by the University (i.e. on-net international, on-net domestic, off-net international and off-net domestic) and summarised by internal destination i.e. group (faculty/department/section), by IP network (Class B, C address) and by protocol (IP protocol, TCP port, UDP port). In addition for each report it was expected to be able to 'drill down' to view summaries by individual user, subnet or IP address. The approach required the supplier to monitor Internet usage for 6 months prior to the development of an equitable traffic management mechanism that could be applied.

Respondents to the RFP were also required to provide solutions capable of applying a variety of traffic management methods in a manner that was equitable (e.g. for students based on the number and type of courses they are enrolled in). In the case of bandwidth traffic shaping the students effective bandwidth may be adjusted according to their enrolment. A combination of quota and traffic shaping was also to be considered such that a user's effective bandwidth would be reduced automatically when their quota was exceeded. Respondents were also requested to detail any additional network hardware required to monitor and manage Internet traffic, as well as to provide schematics of how the hardware proposed would be integrated into the University network.

UTAS recognised that quotas and traffic shaping would only apply to traffic incoming to the University. However UTAS requested that the proposed solution should be capable of applying traffic management both bi-directionally and asymmetrically.

Like many other Universities, UTAS continues to use authenticated proxy servers to provide an audit trail of users' web/ftp usage and it was anticipated that under the proposed solution an un-authenticated proxy server (possibly transparent proxies) would be used such that users would only need to login once before accessing the Internet or other on-line services (single sign-on) mechanism. At the end, the decision was made to abandon use of proxies completely since their use in Web2 era is becoming irrelevant due to dynamic nature of the sites. Significantly the solution was required to be able to provide a per user audit trail for all Internet traffic. A key function of the reporting module being that given an IP address, date and time the system would be able to identify the user responsible for the traffic.

Other requirements listed in the RFP included that all administration and viewing of reports should be via a browser independent web interface and that the user interface for logging onto the Internet and viewing quotas should also be platform independent. Whilst not a requirement, the RFP noted that a solution that could be expanded to provide billing services for the University's PABX and VoIP telephone system would be viewed favourably. In summary UTAS requirements were:

- Monitoring and traffic categorisation along AARNet billing guidelines:
  - Traffic categorisation as on-net domestic, on-net international, off-net domestic and off-net international.
- Summarisation of traffic by:
  - Internal destination i.e. group (faculty/department/section)
  - IP network (Class B,C address)
  - Protocol (IP protocol, TCP port, UDP port)
  - Detail such as individual user, subnet or IP address.
- Compatibility with the University core data network infrastructure built on CISCO hardware. The University's boundary firewall and separate virtual firewalls used to manage the University's DMZ.
- Integration with University authentication services (Active Directory) and 802.1x

2.1 Procurement of an improved monitoring solution

UTAS received a number of responses to its RFP but it quickly became apparent that none of the respondents could

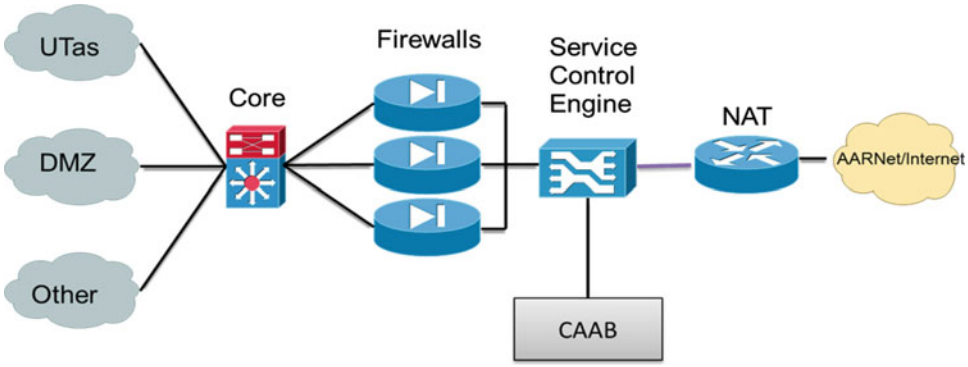

Fig. 1 Functional model of IMS

provide a system that completely met the requirements of the University. As a result a period of negotiation and further investigation was done to identify the solution that could be most easily modified or extended to meet the University's requirements. These investigations led to the selection of TSA Software Solutions, who proposed adapting their Call Accounting and Billing (CAAB) solution. This software was developed for telecommunications monitoring and billing and TSA had proposed to adapt this, via a joint research and development project, to meet the requirements of the University.

System development occurred during 2008, with a pilot rollout occurring at the end of 2008 and during 2009. The solution consisted of a CISCO Service Control Engine undertaking traffic inspection and the CAAB application performing accounting of the traffic (see Fig. 1).

The CAAB system was modified to apply the telecommunications monitoring and billing to network traffic, as per the requirements of the University. In conjunction with this modification to the system, further alterations to system operation were made to enable authentication via Active Directory and 802.1x. Active Directory authentication was delivered by the development of an Internet Access Client (IA Client). The IA Client is an executable application developed for supported computing platforms that authenticates to IMS using Active Directory login credentials, and connects to a heartbeat server to maintain an Internet session for users whilst they are logged in. 802.1x authentication to IMS is handled via connection to the University's wireless system, that utilises Radius authentication.

Clients connecting from non-supported machines connect through a web interface that launches a heartbeat window to maintain the user's Internet session. This solution is very similar to solutions employed by Internet service providers in more public spaces (e.g. hotel lobbies).

The developments made to the CAAB system allow the association of a username and IP address to each item of network traffic entering and leaving the University's network. In essence, this provides complete monitoring of Internet usage which is then able to be reported on in a variety of ways. Development of reports within the IMS occurred in 2009, with due care and consideration being given to the maintenance of user privacy. Access to IMS data is restricted to two positions at the University of Tasmania, those positions being responsible for policy enforcement in relation to IT usage.

Reports developed to meet the University's requirements are sanitised to provide an overview of use to a head of Faculty, School or Department without disclosing the identity of a user. This enables a Senior Officer to be aware of general usage trends within their budget centre, without breaching the privacy considerations of staff and students.

Figure 2 provides a more detailed schematic of the UTAS IMS implementation.

2.2 Functionality of IMS

The monitoring capability of the IMS during the pilot resulted in a significant improvement in the understanding of Internet usage at the University of Tasmania. Further development of the full reporting capabilities is currently underway but UTAS has already used data produced during the pilot in disciplinary investigations with success.

Integration with authentication systems, and in particular the wireless network, has resulted in Internet access that is more user friendly for staff and students as IMS authenticates all connections for a session and allows applications with limited proxy functionality to work correctly. The IMS employs encrypted authentication standards and so has removed a previous issue where Squid authentication was performed using plain text passwords.

During second half of 2010 the IMS will be rolled out across the University of Tasmania, and report development will continue. Currently IMS users can see their usage in relation to a soft quota target and when reporting is fully implemented, users will be able to request an off-line report of their complete activity. Similarly, summary reports will be made available to heads of Faculty, School, and Department so that they may see the volume of data their staff and students are accountable for.

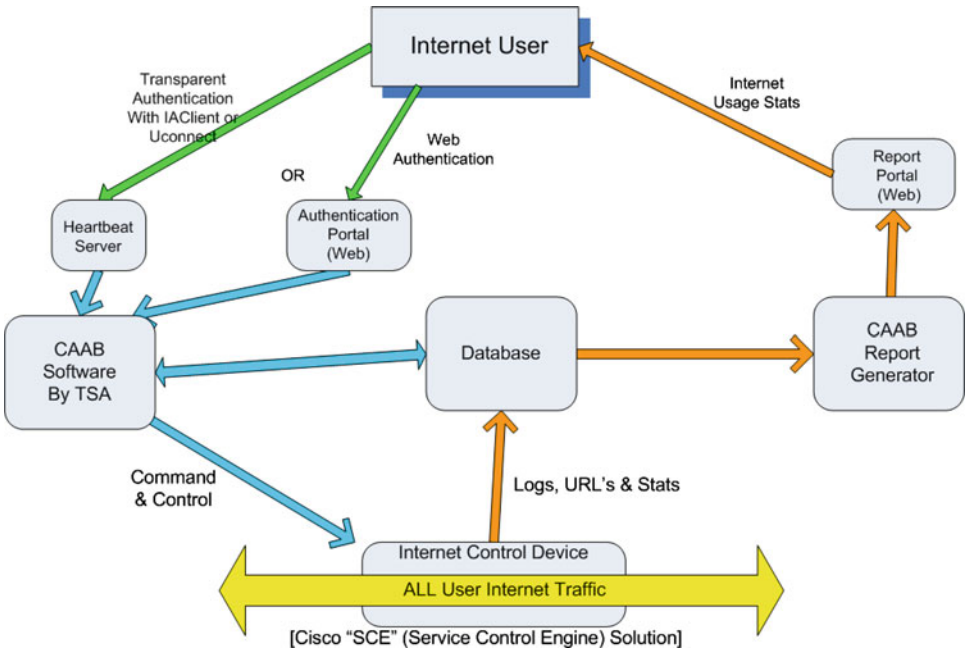

Fig. 2 UTAS Internet Management System

2.3 Future development of IMS

It is anticipated that the IMS will continue to evolve in the future to meet requirements identified from traffic monitoring and management. Concepts such as protocol blocking or limiting will be investigated, as will rate limiting of traffic to sites of low educational value. Consideration will be given to limiting traffic from 'low value' sites with priority (i.e. speed) given to sites of a high educational value. This might see rate limited traffic to for example YouTube and Facebook, with traffic reserved for online journal access. UTAS anticipate that this approach will lead to an improvement in the quality of services (QoS) overall but may require tailoring to overcome some concerns that it could be detrimental to the use of social networking sites as potential relevant and valuable teaching tools.

Similarly it is anticipated that selective blacklists will be applied in future iterations of IMS. The University selectively blocks some social networking sites from selected student labs via proxy restrictions, and these will be incorporated into the IMS. Also student and staff access restrictions as a result of disciplinary action will be implemented into IMS in 2010–2011. These restrictions can include complete access bans, allowing only Intranet access, or white-listing to allow access only to select sites.

2.4 ICT Security policy framework

The introduction of IMS, via the pilot phase and early deployment as analysed in this paper, was conducted with little policy support. Prior to June 2010, University Policy regarding the use of the ICT was focused on user behaviour at the expense of presenting general guidelines around all aspects of ICT Security operations.

In June 2010 the University of Tasmania Council endorsed a revised ICT Security Framework[1]. The ICT Security Framework expands policy coverage to logical/physical controls, access controls and user controls.

Of particular importance to IMS are formal declarations around the collection, management, and provisioning of user information within the University and to external parties. These declarations were made in Policy to adhere with the requirements of the Personal Information Protection Act 2004 [10] which is the overarching legislative document for Tasmanian entities.

The Act defines personal information as:

> *"...any information or opinion in any recorded format about an individual –*
> *(a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and*
> *(b) who is alive or has not been dead for more than 25 years;"*[10]

The monitoring capabilities of IMS clearly satisfy the definition of personal information under the Act, presenting the University with a requirement to adhere to the Personal Information Protection Principles defined in the Act when managing IMS data.

The Personal Information Protection Principles are series of statements regarding the collection, storage and use of personal information. Summarily, the requirement of any

[1] See http://www.utas.edu.au/governance-legal/policy/policy-and-delegation-announcements/announcements/ict-security-framework-approved.

organisation bound by the Act is that personal information collection must be related to a function or activity of the organisation, must be collected by lawful means, and collection must be stated. Use of personal information must be for stated purposes or for purposes where the subject has given consent. Disclosure of information is generally only allowed for stated or authorised purposes, or to law enforcement agencies.

To comply with the Personal Information Protection Principles of the Act, the University of Tasmania included the following statement in the ICT Services and Facilities Use Policy[2]:

> *"All usage of ICT Services, Facilities and Infrastructure will be monitored.*
> *Information related to the usage of ICT Services, Facilities and Infrastructure will be stored and may be used to ensure or investigate compliance with University Policies, Procedures and Guidelines and relevant State and Federal legislation, the University of Tasmania may collect information related to the use of ICT Services, Facilities and Infrastructure.*
> *Further information related to the monitoring of ICT Services, Facilities and Infrastructure, and the usage of information collected, is provided in the ICT Security Policy."*

The immediate intention regarding this statement is to make an overt declaration regarding the status of usage information at the University of Tasmania. The primary purpose as described in terms of 'user' controls is to ensure Legislative and Policy adherence, which largely relates to the use of University ICT Facilities in a legal manner.

The ICT Security Policy expands on the collection of personal information, and the use thereof:

> *"The University of Tasmania provides members with access to ICT Services, Facilities and Infrastructure in support of teaching and learning, research activities, and in support of University business. These Services, Facilities and Infrastructure are provided on condition that members meet the requirements described in the ICT Security Framework.*
> *In order to ensure compliance with University Policies, Procedures and Guidelines and relevant State and Federal legislation, the University of Tasmania may collect information related to the use of ICT Services, Facilities and Infrastructure.*
> *...*
> *Information related to the usage of ICT Services, Facilities and Infrastructure may be consulted to investigate and ensure compliance with legislation and policies, or may be used for the purposes of: operations, maintenance, audit, quality of service, identifying inappropriate, excessive or unauthorised usage and for the purpose of litigation and criminal investigation."*

The ICT Security Policy provides an expanded declaration of the monitoring of ICT usage at the University of Tasmania, and reinforces the primary collection purpose. Additionally the ICT Security Policy declares that personal information may be consulted in an operational capacity.

IMS provides an extremely comprehensive view of user behaviour in relation to Internet usage, and therefore it was crucial that supporting Policy clearly state data collection purposes prior to expanded rollout of the system at the University of Tasmania.

As discussed in this paper, IMS reporting allows for a highly restricted number of staff to view the complete information set. These individuals, the Director, IT Resources, and the ICT Security Officer, act as custodians of the data with the purpose of acting on the primary data collection purpose, Legislation and Policy enforcement. Restricted views of data through the IMS reporting interface allow operational activities to occur as the data become pseudo-anonymised and identification of users and their activities is masked.

The ICT Security Framework provides an important foundation for IMS by disclosing the collection of information to users and stating the primary purpose for that collection.

The University IMS policy processes described above were developed within a broader legal framework that it appears may be about to change in ways that will have a direct impact on the approaches described. In particular, on 30 April 2010, in joint media release Australia's Attorney-General, Hon. Robert McClelland MP and Minister for Foreign Affairs, Hon. Stephen Smith MP announced that Australia would accede to the Council of Europe Convention on Cybercrime [8,9]. No additional information was provided on a proposed timeline and/or any changes to Australian laws to accommodate this accession. However, it is sensible to predict that significant changes will need to happen since the Convention relies heavily on other EU directives and/or conventions, e.g. Directive on Privacy and Electronic Communication [11]. Indeed, it has been already reported [12], that the Australian Federal Government will overhaul its 22 years old Privacy Act [13], in turn forcing individual States and Territories to amend their Privacy Acts. It is reported that this move was in part due to increased awareness of issues arising from recent incidents involving Google's WiFi data collection procedures in several countries, but it can also be argued that the accession announcement will also have contributed to these plans. Following any substantive changes to Australia's legal frameworks it will be necessary for Universities to review their implementations and utilisation of IMS.

[2] See http://www.utas.edu.au/__data/assets/pdf_file/0015/50541/ICfTP-3.1-ICT-Services-and-Facilities-Use-Policy.pdf.

What is already evident is that balancing security, privacy and any need for digital evidence is not likely to become less complex. Perhaps more significantly, it is evident that any changes are likely to take time and leave Universities to work with uncertain or changing legal frameworks that will be at best unhelpful in trying to maintain a suitable balance.

3 Part two: IMS implications: privacy, security and forensic computing

Part one of this paper above presented a short case study covering the technical and organisational setting, the initial call and process of IMS selection, implementation and preliminary evaluation and includes a description of the IMS product.

This part of the paper discusses how decisions pertaining to IMS systems have direct implications for the balance of competing rights, interests and requirements from different stakeholders. This discussion recognises the impact of the changing nature of users' relationships with the Internet and highlights the need for continued vigilance on the part of users, network administrators, service providers and policy makers. This discussion illustrates the dangers of failing to get the right balance and argues for the importance of user education, change management and communication throughout the University and its broader community of users.

It should be noted that this discussion is currently preliminary in nature because the IMS deployment is not complete. It is anticipated that further research will be conducted post-full implementation of the IMS. The authors are also intending to engage with staff responsible for running this system and those who may be involved in the possible future use of this system for the enforcement of legal requirements of the University in regards to privacy, security, copyright management and /or the conduct of forensic computing investigations into alleged criminal, illegal or inappropriate on-line behaviours.

In this context, it is interesting to record the different reactions of staff in two academic schools who participated in the initial IMS roll-out. Academics in one school immediately protested against the IMS citing attacks on 'academic freedoms', 'intrusion to privacy' and 'big brother type' surveillance. These protests occurred prior to the IMS deployment. In the other school, the deployment was done within 24 h from the announcement without any problems or complaints.

One major factor to explain these very different reactions appear to be the education and training provided on the IMS at the two schools. In the school with protests, the memorandum announcing this system started "*The University is moving to a new Internet traffic* **monitoring**[3] *system dubbed IMS (Internet Management System).*" The unfortunate use of the word 'monitoring' at the very beginning appears to have immediately triggered all the protests. In the other school the explanation to staff was more thorough including explanations of security and privacy benefits of the new system to users, and care was taken not to use the word monitoring. Clearly, this word may not be the only reason for academic disquiet about the new system and indeed, it must be acknowledged that the IMS does have a monitoring function that requires a continued scrutiny. It also highlights that user education and change management play an important role in managing the balance of interests and expectations about the issues that such systems generate [5,14].

The protests however, also do illustrate the underlying concerns that academic colleagues have about the management of Internet access. While at one level, these concerns may be able to be 'managed' they are certainly not invalid per se and do require serious consideration on behalf of system implementers and educators. This consideration must acknowledge the limitations of the technical systems that are being implemented. While these systems may be a significant improvement on previous approaches, the nature of the Internet is changing too quickly for any system to be perfect or infallible. The requirement for continued vigilance and openness about the genuine risks that continue exist must also be part of the education of users. More generally while this paper has not assessed the implementation of the IMS against applicable Australian laws, it is useful to note that such a system might well be illegal in certain European jurisdictions, e.g. France and Germany.

These issues will be discussed in more detail below in the sections on Privacy, Security, and Forensic Computing.

Since the deployment of the IMS users have reported positively on the new system. These reports have included:

- An improvement in the responsiveness of web-browsers;
- Renewed functionality of some software packages that previously did not work with the authenticated proxy previously employed by UTAS;
- Very positive responses to the fact that there is now a 'single-sign-on' approach instead of being forced to authenticate each time Internet access was required.

Users have additionally expressed appreciation for the opportunity to view how much Internet traffic they use in any given month (see Fig. 3). This is particularly important in the current uncertainty of not knowing whether there will be quotas/payments or other limitations imposed on their access to the Internet. Many students in particular report that their usage is actually much smaller than they expected.

[3] Bolding added by authors of this paper.

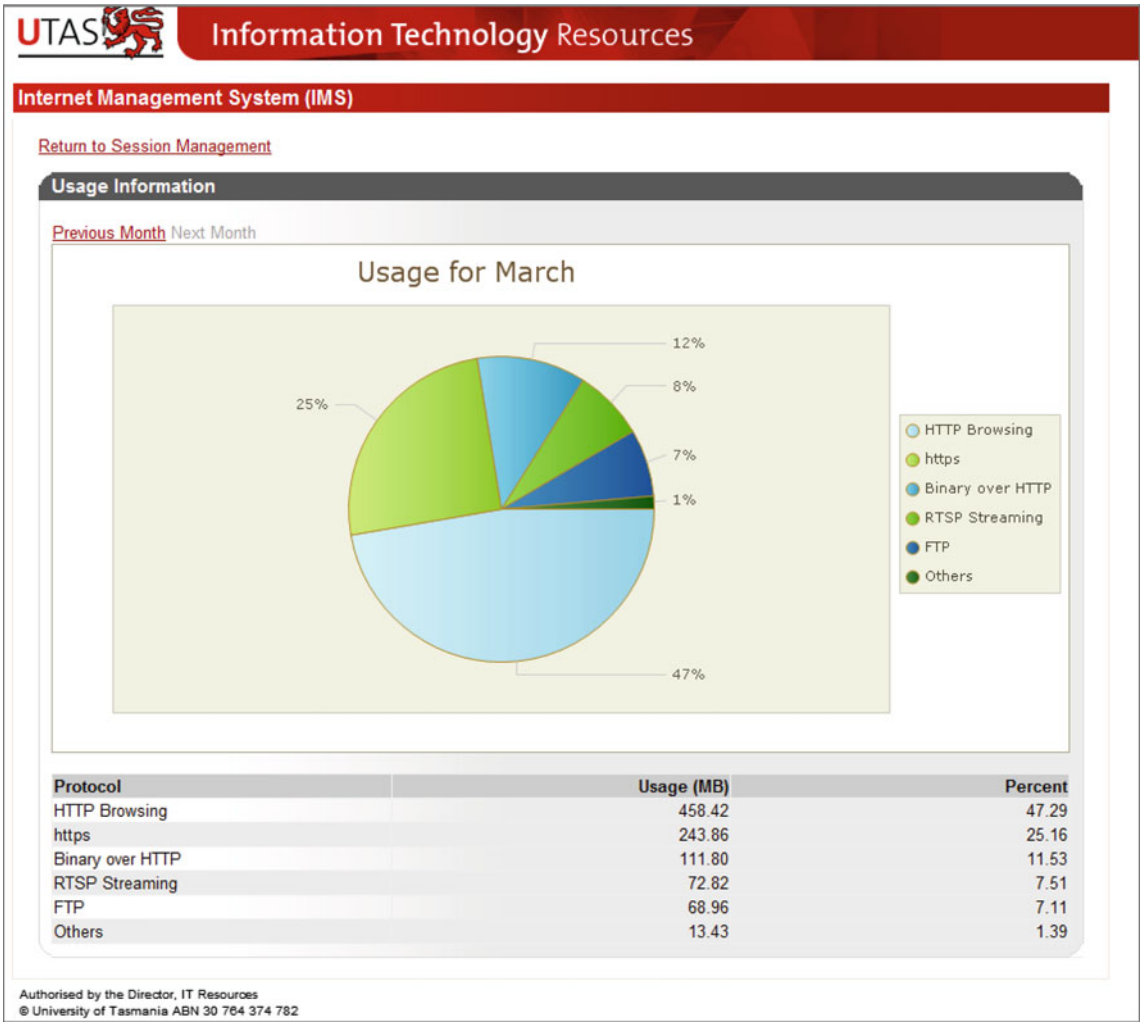

Fig. 3 Example usage report

3.1 Privacy

A comparison of the old system at UTAS and the new IMS reveals that the new system does provide an improved level of user privacy (and security) during on-line browsing. The old system of authenticated proxy used simple authentication where user name and password travelled across the University network in virtually 'clear text', using only base64 binary-to-text encoding. The new system uses authentication against Microsoft Active Directory (AD) and the username and password are not visible 'on the wire' at all, or are visible in an encrypted form.

The data from the old system were kept in several flat files with access to them by several different ICT employees. The new system stores all data in an SQL database. The access to full data is given only to two senior ICT staff responsible for enforcement of ICT policies and sanitised reports are prepared for all other areas. However, concerns over privacy do remain and questions about the reliability of system administrators and policing of their access to this data remain, since anybody with administrative access to the SQL server has potential access to the data. These concerns go beyond any that might be raised by the University's Security Policy Framework as described in Sect. 2.4 ICT Security Policy Framework.

Thus the age old question of 'who polices the police' remains unanswered by the IMS. Indeed, even if the initial protests from some academics with little knowledge of the new IMS might be characterized as 'emotional' it is clear that apart from the risk of privacy abuse from within the University there are potentially even more significant privacy and data protection concerns arising from situations in which the legal action by external parties against the University might lead to the transfer of data to be analysed by unmonitored third parties as it occurred during the 2003 legal action (see 1 Introduction).

In this context, there is enough evidence to suggest the utilisation of pseudonymisation. It is acknowledged that there are reported positive and negative consequences of using pseudonymisation for various data streams in computer security, forensic computing and other related areas[15–23]. However, to address these underlying privacy concerns it would appear that there is merit in exploring the deployment of pseudonymisation.

3.2 Security

The new IMS system provides higher security for users and their data than was previously provided. It also ultimately provides improved security of ICT systems since 'blacklisting' is now much easier to implement. (e.g. In a recent case of phishing e-mails pretending to be from the Australian Taxation Office, the access to the website that was collecting the data was blocked within a few minutes of receiving the first such e-mail, potentially saving many users from disclosure of their taxation details to phishers). Unfortunately, while things have been improved, experience at UTAS suggests that there will always be a small number of users who will fall for such fake e-mails. This appears to be a common problem beyond University environments as is perhaps best evidenced by the continued occurrences of the stereo-typical 'Nigerian Scam'.[4]

The IMS does however continue to face questions over the level of security provided to IMS data. It is also evident that concessions have been made in order to make the system easily deployable and light-weight (e.g. the heartbeat of the client as well as of the web interface use the http protocol). Although only the domain\username and HMAC (Hash-based Message Authentication Code) generated using SHA1 are sent for each heartbeat, it would be preferable to use the https protocol. However, implementing SSL into the client would make it much 'fatter' and that was deemed undesirable. Since the heartbeat is a single http message without response from the server, it might also be possible to use UDP for this communication.

The IMS implementation also initially introduced a minor problem with licensing of access to journals and database providers. Many of these providers license/control access to their sites on the basis of IP numbers or ranges. In the past, all outgoing http and https traffic from UTAS originated from a set of only four IP addresses representing four squid proxy servers in a particular B class address range. Consequently, UTAS had most licenses issued on a basis of this B class range. Without any forms of proxies at UTAS, after full implementation of IMS, traffic now comes from at least three B class ranges. As a result, the providers are reluctant to change to such wide open licensing/control. Initially, several subnets have lost access to these providers. To remedy this, these subnets now use NAT (Network Address Translation) for outside access. This is definitely an undesirable outcome introducing possible security problems and complicating identification of originating computers should outside parties claim cyber-attacks are originating from UTAS. Alternative solution utilising EZproxy[5] is being tested at the time of writing this paper.

3.3 Forensic computing

The IMS is also a typical example of data sets used in post-mortem investigation and raises concerns as expressed by Broucek & Turner[24] that remain unanswered:

> "*In the context of conventional forensic post mortem investigations, privacy concerns may emerge not in relation to the individuals under investigation but rather others whose activities are also part of the data sets being analysed. To date there has been little discussion of the implications of these knock-on effects involving privacy intrusion. While it can be assumed that the data set under investigation is treated in an appropriately secure manner this does not address any knock-on breach of privacy, confidentiality or both. It also provides no mechanism for safeguards against the abuse of this private information by investigators at some future date. In essence this is the age-old problem of who polices the police. More traditionally it is acknowledged that concern with privacy issues adds an extra burden to the work of investigators both in the technical process of forensic analysis and in the presentation of that evidence within the legal system.*"

The data collected by the IMS provide clear links between users logged into the system and computer and network traffic. However, this does not solve the 'last mile' problem [25], in particular in the University environment of heavily shared computing resources, use of NAT and the culture of students who often do not have any or very little understanding of the dangers of Internet access sharing. Indeed, there exists very strong anecdotal evidence of students (and worryingly sometimes even staff) not logging out of computers and/or sharing their usernames and passwords. This in turn provides an opportunity for misuse that would either put the blame on the wrong person, or would pose challenges to prove/defend against in cases of alleged criminal, illegal or inappropriate on-line behaviours.

[4] For an example, see http://www.scamwatch.gov.au/content/index.phtml/tag/Nigerian419Scams.

[5] See http://www.oclc.org/ezproxy/.

4 Conclusion

This paper has presented a short case study on the experience of the UTAS in introducing new Internet Management System (IMS). The case study covered the period from the initial 'call for proposals' through to the partial deployment of the new IMS system.The paper reveals how decisions pertaining to the IMS systems have direct implications for the balance of competing rights, interests and requirements from different stakeholders. More specifically the case study highlighted the impact of the changing nature of users' relationships with the Internet and the need for vigilance on the part of users, network administrators, service providers and policy makers. The paper highlighted the dangers of failing to get the right balance and argued for the importance of user education, change management and communication throughout the University and its broader community of users. The paper also briefly considered how Australia's recent accession to the Council of Europe's Convention on Cybercrime may impact on these issues.

This paper concludes that while the privacy and security of users and their data is clearly improved by the new system, there remain areas for further improvement and vigilance. From a forensic computing perspective, the quality of the data remains questionable and further research and tests need to be completed. The authors believe that these preliminary conclusions may resonant outside of University environments where IMS are in use.

More broadly, this paper suggests that further changes will emerge as IPV6, companies like Google and cloud computing architectures reconfigure individual users relationships with 'their' information and access to the Internet. These developments will continue to transform the meaning of concepts like ownership and control, privacy and freedom of speech within and beyond on-line environments. Without care to balance the interests of different stakeholders there remains a danger of creating an experience of Internet access in an academic environment of 'Big Brother Surveillance' and/or an Internet of 'Self-censoring behaviours'. Alternatively, users may respond to their concerns with a solution such as the mass adoption of encryption to ensure privacy and security of users from prying eyes.

References

1. Sony Music Entertainment (Australia) Limited v University of Tasmania.: FCA 532 (30 May 2003). Federal Court of Australia (2003)
2. Sony Music Entertainment (Australia) Limited v University of Tasmania.: FCA 724 (18 July 2003). Federal Court of Australia (2003)
3. Sony Music Entertainment (Australia) Limited v University of Tasmania.: FCA 805 (29 July 2003). Federal Court of Australia (2003)
4. Sony Music Entertainment (Australia) Limited v University of Tasmania.: FCA 929 (4 September 2003). Federal Court of Australia (2003)
5. Broucek, V.: Forensic Computing: Exploring Paradoxes—an investigation into challenges of digital evidence and implications for emerging responses to criminal, illegal and inappropriate on-line behaviours. School of Computing and Information Systems, PhD, pp. 299. University of Tasmania, Hobart (2009)
6. Broucek, V., Turner, P., Frings, S.: Music piracy, universities and the Australian Federal Court: issues for forensic computing specialists. Comput. Law & Secur. Report. **21**, 30–37 (2005)
7. McCullagh, A., Caelli, W.: Extended case note and commentary: Sony Music Entertainment (Australia) Limited & others v. University of Tasmania & others [2003] FCA 532 (30 May 2003). Comput. Law J. (53). Available at http://www.nswscl.org.au/journal/53/McCullaghCaelli.htm (2003)
8. Federal Government of Australia. http://www.foreignminister.gov.au/releases/2010/fa-s100430.html
9. Council of Europe.: Convention on Cybercrime. In: Europe, C.o. (ed.) European Treaty Series—No. 185. Council of Europe, Budapest (2001)
10. Personal Information Protection Act 2004 (No. 46 of 2004). Tasmania, Australia (2004)
11. European Parliament, Council of the European Union: Directive 2002/58/EC—Directive on Privacy and Electronic Communication. Off. J European Commun L, pp. 37–47 (2002)
12. Bita, N.: Privacy laws get internet update. The Australian. Nationwide News Pty Limited (2010)
13. Privacy Act 1988 (Act No. 119 of 1988). Australia (1988). http://www.comlaw.gov.au/
14. Broucek, V., Turner, P.: E-mail and WWW browsers: a forensic computing perspective on the need for improved user education for information systems security management. In: Khosrow-Pour, M. (ed.) 2002 Information Resources Management Association International Conference, pp. 931–932. IDEA Group, Seattle Washington, USA (2002)
15. Biskup, J., Flegel, U.: On pseudonymization of audit data for intrusion detection. Workshop on design issues in anonymity and unobservability, vol. 2009, pp. 161–180. Springer, Berlin, Heidelberg, Berkeley, California (2000)
16. Biskup, J., Flegel, U.: Transaction-based pseudonyms in audit-data for privacy respecting intrusion detection. Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000), vol. 1907, pp. 28–48. Springer, Berlin, Heidelberg, Toulouse, France (2000)
17. Biskup, J., Flegel, U.: Threshold-Based Identity Recovery for Privacy Enhanced Applications. In: 7th ACM Conference on Computer and Communications Security (CCS 2000), pp. 71–79. ACM, Athens, Greece (2000)
18. Jorns, O., Jung, O., Quirchmayr, G.: Transaction pseudonyms in mobile environments. J. Comput. Virol. **3**, 185–194 (2007)
19. Lundin, E.: Anomaly-based intrusion detection: privacy concerns and other problems. Comput. Netw. **34**, 623–640 (2000)
20. Lundin, E., Jonsson, E.: Privacy vs intrusion detection analysis. The 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99), Lafayette (1999)
21. Lundin, E., Kvarnström, H., Jonsson, E.: Generation of high quality test data for evaluation of fraud detection systems. The sixth Nordic Workshop on Secure IT systems (NordSec2001), Copenhagen, Denmark (2001)
22. Sobirey, M., Fischer-Hübner, S., Rannenberg, K.: Pseudonymous audit for privacy enhanced intrusion detection. In: Yngstrom, L., Carlsen, J. (eds.) IFIP TC11 13th International Conference on

Information Security (SEC'97), pp. 151–163. Chapman & Hall, London, Copenhagen, Denmark (1997)
23. Clayton, R., Danezis, G., Kuhn, M.G.: Real World Patterns of Failure in Anonymity Systems. In: 4th Information Hiding Workshop 2001, Holiday Inn University Center, Pittsburgh (2001)
24. Broucek, V., Turner, P.: Risks and solutions to problems arising from illegal or inappropriate on-line behaviours: two core debates within forensic computing. In: Gattiker, U.E. (ed.) EICAR Conference Best Paper Proceedings, pp. 206–219. EICAR, Berlin (2002)
25. Hannan, M., Turner, P.: The Last Mile: Applying traditional methods for perpetrator identification in forensic computing investigations. In: Conference The Last Mile: Applying Traditional Methods for Perpetrator Identification in Forensic Computing Investigations (2004)