

**To Catch a Cyberthief:
Legal and Technical Issues
Affecting Network Monitoring**

Angus Marshall*, Brian Tompsett†,

Arron Zeus-Brown*, George Chlapoutakis

Abstract

From work on the EPSRC-funded Cyberprofiling project, the authors have proposed an algorithmic approach to profiling of illicit activity online. The model is informed by profiling methodologies from Criminal and Geographic profiling of offenders. A useful basic dataset has been considered and how that data may be collected. The collection of data from existing sources and new sources are outlined. The need for large-scale network monitoring to create a data corpus that provides useful results is highlighted.

The initial work on the project examined the available technology for network data monitoring and evaluated various forms of network "honeypot" which permitted the non-invasive generation of network abuse traffic data. The technical issues of implementing a set of such network monitoring instruments are also discussed.

It is well known and understood, in the network communications industries, that routine monitoring of network usage can provide information necessary to allow network manager to optimise performance and respond to incidents. It is believed that all network devices, worldwide, are at least capable of recording considerable quantities of information about the data passing through them. A single network identifier, typically the Internet Protocol address, is commonly used as the principal key.

In recent times, legal interpretations and opinions on the use of network identifiers as personal identifiers have changed at national and international levels. The authors draw comparisons with other monitoring technologies such as CCTV and wiretaps, and other forensic investigation techniques such as DNA profiling and debate these views from the perspective of technology practitioners and present some further areas for debate.

Preamble

The authors are aware that certain regulatory and legislative bodies have taken a view on the treatment of Internet Protocol (IP) addresses as personal data. They are also aware of opinions voiced by some of those responsible for the implementation of legislation applicable to the control and usage of personal data, particularly in respect of the use of such data for research and law enforcement purposes. As scientists and engineers, the authors have strong views about the nature of network addresses and their usage. They present, here, a discussion of the implications of some of the many views, opinions and stances mentioned above from their perspective as those tasked with implementing, managing, securing and investigating computer networks.

Introduction

The research work which led to this discussion resulted from the realisation that a multidisciplinary approach is required for an effective understanding of approaches to Cybercrime. A computer security specialist may understand how a computer may be vulnerable, and how it may be secured. An Internet security expert may understand how a criminal can exploit computer vulnerabilities remotely; a digital forensics specialist may be aware of how to obtain evidence of how a computer is involved in a crime, and a lawyer can be aware of how the law can apply in that case. A criminologist will apply knowledge of criminal behaviour in aiding the understanding the motivation of the criminal, and thus assist in the detection of perpetrators, and a regulator will have an understanding of how the law is being interpreted. A user of information technology will be aware of how all this criminal activity has affected them.

The collaboration between these groups has enabled the expertise from each area to provide a fresh perspective to the work of others and make advances in the detection of Criminals in an Internet context (Marshall and Tompsett, 2005A). The initial project work was the application of Criminal and Geographic Profiling to Internet Crime, which was named Cyberprofiling (Tompsett et al., 2005). This project proposed techniques for the detection of Internet crime, and the gathering of evidence which would assist in the detection of future criminal incidents as well as assist in the prosecution of those detected (Marshall and Tompsett 2005B). In the process of developing the Cyberprofiling solutions several legal and technical issues were exposed, which are discussed here.

Cyberprofiling

The Cyberprofiling project was a multidisciplinary, multi-organisation collaboration that enabled the pooling of expertise. It involved academic researchers in Digital Forensics, Computer Security, Internet Security, Internet Crime, Criminology, IT Law, The Regulator, Law enforcement and IT users. These were specifically represented by The University of Teesside School of Science and Technology, The University of Sheffield School of Law, The University of Hull Department of Computer Science, The Office of the UK Information Commissioner, Humberside Police, North Yorkshire Trading Standards Digital Evidence Recovery and Internet

crime Centre and C. Spencer Ltd. The project was funded by the EPSRC as part of their “Think Crime” initiative in conjunction with the Home Office.

In that project the available sources of data on Internet crime were examined, particularly the existing large databases which could be used (Tompsett and Desai, 2006). The researchers also considered what further data would be required to perform the techniques of criminal and geographic profiling that would be performed in non-Internet crimes. The project produced a prototype of a network data capture appliance, which identified anomalous traffic and recorded the incidents for later pattern analysis. The project showed how the value of profiling and the nature of the tools and techniques that can be employed.

Beyond the initial phase of the project, there is a need to deploy the data collection appliance and start to build a corpus of data. Initial work also indicated predictive models that can be employed (Marshall, Tompsett & Moor, 2006; Marshall, Tompsett & Semmens, 2007).

A representative of The Office of the UK Information Commissioner identified that there could be Data Protection issues if the data were stored in their raw format, and some form of anonymisation would be required (Tompsett and Prior, 2006). A workable prototype solution to the anonymisation problem was developed which allowed for the anonymisation to be reversed should it be required for forensic purposes. In the discussions on the data protection aspect of the work it became clear that the issue of what is personal data in an Internet context is not as straightforward as appeared in guidance from the regulator.

Data Collection

Much of the data useful for Cyberprofiling are already available in the form of log and network traffic files produced as part of normal computer and network operations. The problem in using this as the sole source of profiling data is the variability and reliability of the datasets. These are often incomplete records in various formats. What is required is an extract of this data, which looks at specific aspects useful for the criminal profiling. The Cyberprofiling project extracted the necessary components from these data sets and combined them with that obtained by its own data collection appliances in a common format (Tompsett and Desai, 2006).

The issue of what to collect and where to collect it was addressed in this project. It might appear that data should be collected at places where internet traffic flows, in order to obtain the largest sampling. The nature of the internet means that it is not possible to sample the flowing of data at data switching nodes, simply due to the wide distribution of the network, the wide ownership of the network infrastructure, the enormous volume of data and the speed at which data flows.

The project placed monitoring appliances at terminal nodes in the internet, as regular computers in an application environment and monitored those that probed, or trespassed on these computers. This information generated a good profile of those who are regularly using computers inappropriately. The technology for providing these monitoring nodes is known as a Honeypot.

Several Honeypot types were evaluated and the most suitable selected (Tompsett, 2008) for use as a data collection appliance. The end result of this stage of the project was a tool which could be seen as the internet equivalent of a CCTV surveillance system to monitor some quiet street or alley. However, before such an appliance can be widely deployed from crime detection and/or prevention it is essential that issues of privacy and legality relating to such data collection or "Dataveillance" are explored (Tompsett and Prior, 2006).

Surveillance

The art of surveillance has been practiced for many years even as far back as Sun Tzu's The art of war. Written in the fifth century BC, this contains a chapter on the use of agents or spies to gather data and observe the enemy before attack :

"故曰：知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。
(故曰：知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。)"

which can be translated as :

"So it is said that if you know your enemies and know yourself, you will fight without danger in battles. If you only know yourself, but not your opponent, you may win or may lose. if you know neither yourself nor your enemy, you will always endanger yourself."
(Tzu, Zi & Giles, 2006).

However, Sun Tzu's perspective was primarily that of a general using covert surveillance to obtain an advantage in battle. When considering any form surveillance, be it overt or covert, it is worthwhile noting the public's attitudes towards the general concepts of surveillance and the need for it.

The first reaction is generally in support of surveillance using the phrase "if you've done nothing wrong, you've nothing to fear". Thus it appears there is an acceptance of monitoring as there is a belief that it provides a benefit with little or no scope for misuse or misinterpretation. Conversely, another group tends to respond with "If I've done nothing wrong, why are you watching me?", indicating a general mistrust of any intrusion into personal freedom.

Many forms of surveillance take an *overtly covert* approach, such as the monitoring of credit card usage or loyalty card usage. However another common practice with CCTV is performed by providing a notice or standard paragraph in a contract. Because these have become commonplace and largely unavoidable, the subjects of the surveillance tend to either ignore or accept the surveillance being used, albeit grudgingly, as an unavoidable consequence of certain activities in some cases. The use of CCTV as overtly covert surveillance has been considered by the UK Information Commissioner and is dealt with by the CCTV Code of Practice (2000) (French, 2000), effectively allowing CCTV to be deployed as a form of data collection in public places under the terms of the Data Protection Act (1998). Data subjects are made aware of the existence

of the data gathering & processing system through the use of prominent notices. The CCTV Code of Practice written is not intended to cover :

- Targeted and intrusive surveillance - see Regulation of Investigatory Powers Act 2000.
- Surveillance techniques used by employers to monitor employees contract compliance.
- Security equipment installed for home security purposes – exempt virtue sec 36 of DPA 98.
- Cameras used by the broadcast media for purposes of journalism.

This thus leads to the key issues regarding the DPA 98 and CCTV operation :

1. Legitimate basis for processing images (i.e. valid reason to have CCTV in operation).
2. Systems operation being notified/registered with the Information Commissioner.
3. Signage being appropriately placed on entering a ‘gated’ CCTV area.
4. Systems being overt (a system without signs = a covert system)

Given the above, anyone wishing to implement CCTV monitoring, must first answer the question - "does the system's data controller have a legitimate reason in law to conduct the surveillance?".

If we consider a public location such as a town or city centre the implementation will rely on the Paragraph 5(d) of the schedule 2 of D.P.A. 98 :

“In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.” (Data protection act schedule 2, 1998, 3)

This refers to the processing of surveillance material is for the exercise of any function of a public nature exercised in the public interest. These purposes include prevention and detection of crime, apprehension and prosecuting of offenders (sec 29 DPA 98) or public/employee safety.

It is worth noting, however, that case law (Durant vs. FSA, England, 2003) has limited the scope of the protection provided by section 7 of the Data Protection Act 1998 in that any one recorded by a surveillance device should be able to request copies of said data, though this may be difficult to comply with due to volumes of data and the possibility that others may be "in frame" and identifiable at the time in question.

If the DPA and CCTV model, discussed above, is applied to Dataveillance it may be found that many people are currently performing tasks which are regarded as accepted practice, but which appear to be in violation of the Data Protection Act (1998) and the principles of the CCTV Code of Practice. For example, the monitoring of network traffic can be performed to protect the

network and prevent crime, but is also routinely carried out to responsibly manage and secure publicly accessible networks. In such circumstances, should these network managers have applied for authority under the Regulation of Investigatory Powers Act Covert Surveillance: Code of Practice Order 2002 ? An argument could be made for this as no signage is displayed to the network users whose data are being collected. Similarly, a Section 7 request should be able to be made so that there is, not only compliance with R.I.P.A. but also with D.P.A.. That, however, relies on the supposition that an IP address is a truly personal identifier or even a temporary personal identity token.

IP Addresses as a Personal Identifier

IP (Internet Protocol) addresses have been increasingly viewed as a personal identifier, linking not just an individual computer to a network, be it a local area network or the global Internet, but also the individual who operates that computer. However, this view is not without its issues, arising both through the theory behind IP addressing in general and through the differences in the definition of privacy between the countries using the Internet addressing system.

According to the Internet Engineering Task Force's RFC (Request for Comments) 791 (Postel, 1981, pp. 2), an IP address is defined as an address identifying an individual computer on a private (local area) or public (Internet) network to facilitate data transfers from and to that computer. RFC 791 further notes that the addressing scheme must allow for multiple addresses to be issued to a single computer (Postel, 1981, pp. 7).

Furthermore, IP addresses can be assigned to a computer either dynamically, where, according to RFC 2131 (Droms, 1997) a "leased" or temporary address is assigned randomly from a list of available IP addresses (address block) an Internet Service Provider is given, or statically, where the IP address is permanently assigned by the Internet Service Provider to a device.

In use, the IP addresses are used by the network layer of the Internet Protocol stack to determine logical routing between network devices and not all packets moving between two nodes will follow the same route. IP addresses are contained in the "header" section of a network layer packet to provide sender and destination information. The remainder of the packet is an encapsulation of the packet produced by the layer above it (transport layer, TCP, UDP etc.), with its own encapsulation of data from a higher layer (application layer, HTTP, SMTP, etc.). Thus, at the network level, the IP address provides a logical identifier for an endpoint of the network connection. IP packets are further encapsulated into datagrams by the particular carrier network implementation (e.g. ethernet, token ring, avian carriers) present at each stage of their journey. Thus one IP packet may occupy several different datagram types during its journey. Data may be transformed, intercepted and monitored at each layer of the Internet stack.

Personal identification and packet content

Use of cyberprofiling methods (Tompsett et. al, 2005), may allow related patterns of behaviour to be identified where complete records of packets have been retained. By examining packet content as well as packet headers/routing information it may be able to reconstruct complete communications sessions and identify features which are common to several distinct sessions. In this situation, the monitoring may be subject to more than just legislation affecting the control of personal data. Since the contents of the packets are being examined, it may well be subject to communications interception controls. Without the packet content, though, the profiling and session reconstruction cannot be completed and the related sessions cannot be identified.

Thus there is a conflict – in order to have any chance of identifying related sessions, let alone the individuals responsible, (Zeus-Brown et al, 2007) more data is required than are present in simple logs - complete packet content is required, but this is almost certainly not permitted unless communications interception authority has been granted.

Ahmad & Ruighaver (Ahmad & Ruighaver, 2003) have shown that it is necessary to capture full packets in order to detect and thoroughly analyse instances of network abuse and/or misuse and have shown how audit logging can be deployed at "border control" points in networks to good effect. However, in the development of new internet forensic investigation techniques, Carrier & Shields (Carrier & Shields, 2003) have shown how access to address data is a requirement for the forensic analysis of network traffic in order to detect misuse or abuse, but that inspection of packet content is not required until full analysis of an incident is to be performed. Taking the two outcomes together we can state that it is necessary to have access to full packet content during the "post-mortem" stage as the totality of the incident cannot be understood from address data alone, but that the address data are sufficient to allow detection of an incident without identifying the perpetrators and the exact nature of the incident. Address data does not identify the applications in use.

Legal and regulatory views of IP addresses

In 2001, the Information Commissioner cited the difference between Dynamic and Static IP addresses as the predominant reason for the inability to consider IP addresses in general to be included in the Data Protection Act 1998's coverage (L. Townsend and R. Jay, 2007).

The US federal regulations on public welfare and human services (U.S. Government Printing Office, 2002) began, in 2002, to identify IP addresses as one of the data elements about an individual to be considered as "personal information".

Recently, both the EU and the US have updated their definitions of personal identifiers to include the use of IP addresses (M.A. Marin and B. Chatain, 2008).

The EU Data Protection Working Party, in the press release of the Article 29 (Article 29 Data Protection Working Party, 2008), updates the European Data Protection Act to include IP addresses as personal identifiers to be covered by the DPA framework. Their justification for the amendment of IP addresses cited is the increasing use of search engine's retention of IP

addresses, the resulting profiling performed by the search engines themselves and the increasing use of individual users' search engine histories and profiles created by intelligence services of the countries the individuals reside in. More specifically they state that :

“Search engines fall under the EU Data Protection Directive 95/46/EC if there are controllers collecting users' IP addresses or search history information, and therefore have to comply with relevant provisions.” (Article 29 Data Protection Working Party, 2008)

In the case of the US, a recent court case, State versus Reid (C.J. Rabner, 2008) in 2008, created a precedent that extends the view of IP addresses as personal identifiers, stating that the use of a Internet Service Provider-assigned IP address is a requirement for a user's connection to the Internet and that since the user is accessing the Internet from the privacy of their own home, they should expect their actions to be confidential. The case furthermore identified that Internet Service Providers as the default place where information linking individual users to individual IP addresses are linked.

Permanent VS. Temporary Personal identifier and tokens

The idea of personal identifier is commonly thought of as something to uniquely distinguish a person or a physical characteristic of the person such as the name or photographic image. Such identity tokens (Table 1) can be thought of as *permanent* personal identifiers as they are always be associated with that person with no time limit on their validity.

A wired telephone number could be thought of as a *temporary* Personal Identifier in that the Identifier is associated primarily with an address or location, but for a time limited duration (eg. the length of a phone call) may become associated with the person using the telephone, this is due to addition identifiers being invoked such as the users voice and name.

However if one then moves to the e-environment and takes an IP address that is assigned by the ISP (Internet Service Provider) the token becomes *dynamic* as it can be either *permanent* or *temporary* depending on the ISP and connection type. Even at this point the IP address is associated with a network device rather than a user.

Permanent	Fingerprint, DNA profile, Retinal pattern, Iris pattern, etc
Temporary	Name, Work Payroll Number, Passport Number, Nickname, etc

Table 1: Other Permanent and Temporary Identifiers

Network Entity identifier vs. Personal Identifier

In a conventional wired telephone network (aka a "land-line" network), the primary identifier available for the users of the network is the telephone number. Conventionally, after dialling a number and hearing a person answer at the other end, it is necessary to engage in some protocol in order to either identify the person who has answered or have the call session transferred to the person required. In this situation it seems, to the authors at least, that it is generally acknowledged that the phone number does not and cannot identify the person at the other end of the line, hence the need for the additional stage prior to the main communication commencing.

Examining the system in more detail allows us to pick out three distinct identifiers in the system, each of which must be present at both ends in order for the call to be established. Firstly, we have the physical connection from exchange to handset (shown as the "exchange line" in Table 2 below). This uniquely identifies the hardware to be involved in the call. Then a valid customer account, associated with the exchange line, must be present to allow service to be provided and charged for. This is simply an accounting process and records the fact that the person responsible for the account is likely to pay any associated bills. It does not, of itself, indicate that they have exclusive access to the handset. Finally, we have the phone number which is, historically, a structured number used to control exchange switching and hence provides embedded logical call routing information to allow the network to establish a connection from one handset to another.

In mobile, or cellular, telephone networks we have some equivalent concepts. The International Mobile Equipment Identifier (IMEI) is a unique identifier for each handset and allows the network to distinguish between physical pieces of equipment. The IMSI (International Mobile Subscriber Identifier) would be more accurately an IMAV (International Mobile Account Verifier) and allows the network to verify that a SIM card which is credit-worthy is present in the handset (this can be pre-paid and thus have no record of ownership). Finally the phone number provides logical information about which of the many network providers is responsible for each end of the call and allows the network to establish a logical route between the two, as before.

<u>Land-Line</u>	<u>Mobile</u>	<u>Internet</u>	<u>Building / Post</u>	<u>Vehicle</u>	<u>Purpose</u>
Exchange Line	IMEI	Mac Address	Grid Reference	VIN	<i>Hardware ID</i>
Account	IMSI	Network Credentials	Postage Stamp	Tax, MOT, Insurance	<i>Authority to Use System</i>

Phone number	Phone number	IP Address	Postal Address with postcode	Registration number	<i>Structured Logical identifier</i>
--------------	--------------	------------	------------------------------	---------------------	--------------------------------------

Table 2 : Identifiers present in communications systems

In the case of Internet identifiers, most equipment is now based around the IEEE802.3 ethernet standard (IEEE 802.3 Ethernet Working Group, 2005). This requires each piece of equipment to have a Medium Access Control (MAC) address, which is used to identify the hardware at the local physical level. Because users are free to change equipment at will (and thus change MAC addresses), service providers allocate them something like a username and password which are used to associate network sessions with a customer account for billing or other purposes. A successful logon with these network credentials grants access to the ISP's network and allows an IP address to be allocated for the session in order to allow logical traffic routing to take place.

This type of structure (physical object ID, authority to use the system, logical identifier) is common in many other environments. Some further examples are given in Table 2.

From this, the authors believe it is consistent to consider an IP address as no more a personal identifier than a telephone number - i.e. not at all. The IP address merely allows routing between equipment to be carried out, once sessions have been established, and cannot identify a person without the addition of some form of identification protocol (as in the start of a phone call), or database lookup. Even when the person responsible for paying the ISP bill can be identified, this does not equate to the person responsible for a session.

Scenario

In order to understand some of the problems created by the treatment of IP addresses as personal identifiers, consider the following scenario, typical of that found in most smaller business and domestic networks.

Internally, the network consists of several machines, typically one or two per person authorised to use the network, connected together via a switch and linked through an ADSL device to a commercial Internet Service Provider (ISP). The ISP has assigned a single IP address to the ADSL device as the single network device connected to its network. This ADSL device presents the assigned logon credentials to activate its connection.

The group of machines on the internal network are allocated private IP addresses from one of the networks defined as available for private use by RFC1918 (Rekhter, 1996) and thus not permitted to appear on the public Internet.

Using a port-mapping method, the ADSL device acts as a network sharing node and performs Network Address Translation (NAT) or proxy functions, converting packets from the internal

network into packets which are permitted on the public Internet. Packets received from the Internet are checked by the ADSL device to determine where their true destination is and converted back into something appropriate for the internal network. Thus, to the outside world, all traffic to and from the machines on the internal network appears to come from the single ADSL device with its lone IP address allocated by the ISP.

The ADSL device's IP address may change from time to time as the ISP is free to issue and re-issue IP addresses from its allocated range at will. Its network identity (Marshall & Tompsett, 2005), therefore, may change over time. Thus, unless we have some additional information, we are unable to determine precisely which subscriber's network is responsible for network traffic at any time.

Even if we can determine the network responsible (based on the ISP allocated IP address), we cannot fully determine which node within the private network, represented by the single IP address, is responsible for any packet. Since the port-mapping tables within the ADSL device are transient and all machines have the same range of ports available, it is not possible to identify an individual machine in the network by simple inspection of packets collected by external network monitors.

Issues arising from this scenario

The presence of NAT and/or proxies creates a situation where traffic from multiple machines, controlled by several people, is multiplexed into a single stream which appears to come from a single node, identified by a single IP address.

In this respect, it is no different to the postal system. Each person in a building may send letters by placing them into a public mailbox, from which they are collected and multiplexed by the postal system itself. Letters are delivered to the house based purely on street address and, only when they have entered the building, are they demultiplexed for delivery to the individuals identified on the envelope by some means (not necessarily by name – it may be by office number, department or some other identifier).

The street address, therefore, does not allow us to identify the person within the building without access to the internal demultiplexing table (which is the NAT table used by the ADSL device in our scenario).

Even where only a single machine is connected to the ISP we still have the problem that there may be multiple users of that machine and, without external corroboration, we cannot state who is using it any time purely from inspection of IP addresses in use. Even a "post-mortem" examination of the storage devices on the computer for forensic purposes cannot identify who was using any particular logon credential at a particular time, merely that the account was in use.

Conclusion

The position that profilers of internet crime are placed in is contradictory, and perhaps needs further resolution. They look at criminal activity whose prime key is that of the Internet (IP) Address. The IP address is not considered sufficient to identify an individual for the purposes of evidence in a prosecution, yet at the same time legal restrictions indicate that the IP address is a personal identifier and therefore their data storage must be restricted. Whilst the authors feel constrained to not store this information for the purpose of profiling, those that operate and manage the internet appear to freely use and store these same IP addresses and related information despite the legal position. If such information was not usable by the network operators, the operation of the whole internet could effectively cease. In some senses the whole operational management of the Internet might have been ruled out of legality, and only law enforcement and crime detection have been affected.

By comparing this conundrum with similar technical aspects of other communication technologies, such as land-line telephone, mobile telephones and so forth, the authors can see that there are many parallels to the technical identification of devices and individuals that are much more distinctly understood in both the technical sense and the regulatory position. It is almost as if the regulators were given different technical advice regarding one technology, as another.

Comparing and contrasting the position of internet monitoring to that of other surveillance technology, such as CCTV, shows some similarities to surveillance, but also clear distinctions, which are not currently reflected in the legal and regulatory environment.

We conclude that, although the lawyers and regulators might be clear on what can be classified as personal information in an internet record, we believe that there is a degree of contradiction in the arguments that lead to this position. We propose a more logical position that still ensures the correct degree of data protection, yet makes more sense from a criminal profiling and evidential perspective. An IP address on its own does not identify an individual, or the actions that they are performing on the Internet.

Bibliography

1. A. Ahmad and T. Ruighaver , *Design of a network-access audit log for security monitoring and forensic investigation.*, in C. Valli & M. Warren, eds, 'Australian Computer, Network & Information Forensics Conference', (School of Computer and Information Science, Edith Cowan University, Western Australia, 2003). <http://dblp.uni-trier.de/db/conf/ausforensics/ausforensics2003.html>.
2. Article 29 Data Protection Working Party, *Press Release: Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data*, (European advisory body on data protection and privacy, 2008), On-line: <http://ec.europa.eu/>

justice_home/fsj/privacy/news/docs/pr_18_19_02_08_en.pdf, Last seen: 13/06/08

3. B. Carrier and C. Shields, *The session token protocol for forensics and traceback*, ACM Transaction on Information Systems Security 7(2004): 3, 333–362.
4. *Council Resolution of 17 January 1996 on the lawful interception of telecommunications; Interception of telecommunications: recommendation for a Council Resolution in respect of new technology*, ENFOPOL 98, 10951/98, 3.11.98 and ENFOPOL 98 REV 1, 10951/1/98, 4.11.98
5. *Draft Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, JUSTPEN 108, 13144/98, Limité, 19.11.98; PC Magazine, January 1999.
6. R. Droms, *Dynamic Host Configuration Protocol*, (Defense Advanced Research Projects Agency, 1997), On-line: <http://tools.ietf.org/html/rfc2131>, Last seen: 13/06/08
7. *Durant vs. FSA, England*, 2003 Computer Law & Security Report 22 (2006): 4, 2006, pp.320-325
8. *Data protection act, schedule 2 , section 5, p2 1998* On-line: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_10#sch2 Last seen 18/06/08
9. *Data protection act, schedule 2 , section 7 1998* On-line: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_10#sch2 Last seen 18/06/08
10. *Data protection act, schedule 2 , section 29 1998* On-line: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_10#sch2 Last seen 18/06/08
11. *French, E OotUKIC, CCTV Code Of Practive online:2000* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf, Last seen: 18/06/08
12. IEEE 802.3 Ethernet Working Group, *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*, (IEEE Computer Society, 2005), <http://standards.ieee.org/getieee802/802.3.html>, Last seen: 18/06/08
13. M.A. Marin and B. Chatain, *Do internet companies protect personal data well enough*, (European Parliament Press Release, 2008), On-line: http://www.europarl.europa.eu/news/expert/infopress_page/019-19258-022-01-04-902-20080121IPR19236-22-01-2008-2008-false/default_en.htm, Last seen: 13/06/08
14. A.M. Marshal and B.C. Tompsett, *Silicon Pathology ? The Future of Forensic Computing*, Science & Justice 44(2004):1, pp43-50, Forensic Science Society, Harrogate

UK, Jan. 2004.

15. A.M. Marshall and B.C. Tompsett, *Identity theft in an online world*, Computer Law and Security Report 21(Elsevier, 2005), pp128-137.
16. A.M. Marshall and B.C. Tompsett, *Digital Evidence Workshop*, Forensic Science Conference, HE Academy Physical Science Centre, Lincoln, 7th July 2005
17. A.M. Marshall and B.C. Tompsett, *Working with External Partners*", Computer Forensics Workshop, Higher Education Academy for ICS, Northumbria University, 18th November 2005.
18. A.M. Marshall, B.C. Tompsett and G. Moor, *Criminalisation if the Internet: an Examination of Illegal Activity Online*, 4th European Academy of Forensic Science Conference, June 2006, Helsinki.
19. A.M. Marshall , B.C. Tompsett and N.C. Semmens, *Towards an Automated Online Detection and Profiling System*, "Crime and Justice in an Age of Global Insecurity", British Society of Criminology, Mannheim Centre for Criminology, London School of Economics, 18-20 September 2007, p.111.
20. J. Postel (Ed.), *Internet Protocol*, (Defense Advanced Research Projects Agency, 1981), On-line: <http://tools.ietf.org/html/rfc791>, Last seen: 13/6/08
21. C.J. Rabner, "*State of New Jersey v. Shirley Reid (A-105-06)*" (State of New Jersey, Argued 2007, Decided 2008), On-line: <http://www.judiciary.state.nj.us/opinions/supreme/A-105-06%20State%20v%20Shirley%20Reid.pdf>, Last seen: 13/06/2008
22. Y. Rekhter et.al., *Address Allocation for Private Internets*, RFC1918, 1996, The Internet Society, <http://rfc.net/rfc1918.html>
23. *The Regulation of Investigatory Powers Covert Surveillance: Code of Practice Order, section 7*, 2002
24. B.C. Tompsett, A.M. Marshall and N.C. Semmens, *Cyberprofiling*, Computer Network Forensics Workshop, IEEE Securecomm, Athens Sep 2005.
25. B.C. Tompsett, A.M. Marshall and N.C. Semmens, *Definitions of Cybercrime Technology - proposals from an observational study*, 4th European Academy of Forensic Science Conference, June 2006, Helsinki.
26. B.C. Tompsett and A. Desai , *The use of Internet Databases in Analysis and Evidence Collection*, Advances in Computer Security and Forensics Conference, Liverpool, July

2006.

27. B.C. Tompsett and S. Prior, *Problems of Privacy, Security, Identity, Integrity, Legality and Confidentiality in Internet Crime investigation and evidence collection*, European E-Crime and Computer Evidence Conference, Nottingham, Sep 2006.
28. B.C. Tompsett, *Cyberprofiling: The role of traffic monitoring Honeypots*, Emerging Advances in Digital Evidence Developments Conference, University of Teesside, 7th March 2008.
29. L. Townsend and R. Jay, *IP addresses and the Data Protection Act*, (Manchester, Pincent Masons: Out-law.com, 2007), On-line: <http://www.out-law.com/page-8060>, Last seen: 13/06/08
30. S. Tzu and S. Zi and L. Giles, *The art of war: Chapter 13*, (Filiquarian Publishing, 2006)
31. U.S. Government Printing Office, *Title 45 - Public Welfare and Human Services, Part 164: Security and Privacy*, (U.S. Government, 2002), On-line: http://edocket.access.gpo.gov/cfr_2002/octqtr/45cfr164.514.htm, Last seen: 13/06/08
32. A.M. Zeus-Brown, A.M. Marshall and B.C. Tompsett , *Remote Victim Support in the Digital World: The Profiling of Computer Systems and attacks, p.161, "Crime and Justice in an Age of Global Insecurity"*, British Society of Criminology, Mannheim Centre for Criminology, London School of Economics, 18-20 September 2007