Development of a Legal Framework for Intrusion Detection

Steven R. Johnston, CISSP

Communications Security Establishment
P.O. Box 9703
Terminal
Ottawa, Canada K1G 3Z4
Steven.Johnston@cse-cst.gc.ca

Abstract. To meet demands for increased interconnectivity, efficiency or competitiveness, organizations increasingly rely on technology. This trend creates significant opportunities to improve service delivery and to move into new areas of endeavour. But reliance on an inherently insecure infrastructure exposes organizations to a constantly evolving threat environment. Not only has the nature of the threat changed, so too has the scope of the protection problem. Protection of information systems is now seen as a component of national security. As organizational assets move online, so does the threat. Key sources of threat information are now online, including within the network communications themselves. This puts organizations in a position where they must monitor network communications in order to obtain intelligence, indications and warnings of intrusions and evidence to support criminal prosecution as appropriate. One method of performing this monitoring is through the use of intrusion detection systems (IDS). However, this may involve the monitoring of private communications, which introduces a number of legal (privacy and criminal law) concerns. While existing legislation adequately addresses interception by S&I and law enforcement agencies, they generally fail to address interception of network traffic by other public or private sector organizations. This paper seeks to identify and discuss some of the key legal issues affecting the development of a general legal framework for intrusion detection for network protection.

Keywords Anti-terrorism law, criminal law, interception, intrusion detection, privacy, private communications, wiretap

1 Introduction

Organizations of all types, in both the public and private sectors, are increasingly dependent on information technology. This dependency results from demands for increased interconnectivity, efficiency or competitiveness – on the part of the organizations themselves and/or their clients. These organizations have increasingly

A. Wespi, G. Vigna, and L. Deri (Eds.): RAID 2002, LNCS 2516, pp. 138-157, 2002.

been turning to information system technology for a variety of purposes: e-commerce, e-government, and improvements in information access and sharing among others. Reliance on an inherently insecure infrastructure exposes organizations to a variety of new threats. They must now contend with new cyber-threats such as fast-spreading malicious code and criminal hacking.

The scope of the protection problem has also dramatically increased over the past few years. Protection of computer systems and networks has been an issue of concern for some time. In the last few years, however, the protection of these same systems and networks has come to be viewed as a component of national security. This is due in large part to the work of the President's Commission on Critical Infrastructure Protection (PCCIP), which broadened the definition of national security to include protection of critical infrastructures[1], one of which is the telecommunications sector. Arguably, the telecommunications sector is the most important of the sectors, as all of the others are dependent in some way or another (many of which may not be well understood) on telecommunications.

Traditionally, the emphasis of the protection effort has been on the use of cryptography, firewalls, anti-virus applications and so on. Although this is still very important, greater emphasis is being placed on detection of and response to anomalous events – in recognition of the fact that perfect protection is impossible to achieve. A key element of this strategy is the use of intrusion detection systems IDS), which examine network or host activity to detect indications of malicious activity. However, this may involve the interception of personal or private information, which introduces a number of legal (privacy and criminal law) concerns.

2 Aim

The ability to copy, save and/or log personal information transmitted over a network exists in technologies that are already in widespread use, such as firewalls, servers, and anti-virus software. Indeed, logging of personal information is a far easier proposition in the context of these network infrastructure and security administration tools. The implications of criminal and anti-terrorism legislation are thus not limited to IDS alone, however, this paper will focus on their application to intrusion detection systems.

It is the intent of this paper to examine key provisions of criminal and anti-terrorism legislation, and examine some of the implications for the use of IDS in protecting computers and networks. Reference will be made to legislation from Australia, Canada, the United Kingdom and the United States in order to demonstrate that these are issues of general interest. It is not the intent of this paper to substitute

[1] Critical infrastructures have been defined as " infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security." Anonymous, "Critical Foundations: Protecting America's Infrastructures", The President's Commission on Critical Infrastructure Protection, October 1997, page 19. Although the actual delineation of these infrastructures varies somewhat from country to country, it is generally agreed that critical infrastructures include energy, banking and finance, transportation, water and sewage, government services, emergency services and telecommunications.

for considered legal advice. The opinions expressed in this paper are strictly those of the author and do not reflect the position of the Communications Security Establishment (CSE) or of the Government of Canada (GoC).

3 Interception Requirements

The manner in which public and private sector organizations conduct business and offer services to their clients has changed dramatically over the past several years, as organizations move to e-business, e-government or any other form of online activity. An increasing percentage of organizational assets are moving online, stored in file and mail servers, data warehouses and storage area networks. These assets include financial, medical or personnel records, strategic plans, and trade secrets – all of which represent some of the organization's most valuable assets. Similarly, business communications are increasingly carried by networks of one form or another.

Individuals and organizations that pose a threat to these assets are also moving online. This is partly because this is "where the money is". It is also partly because the use of these technologies confers flexibility, speed and anonymity on their activities. Cyber-threats are difficult to anticipate (other than in a generic way), detect, verify and trace. As the threat is increasingly cyber-based, information about the threat can also be found online. Hacker websites, e-zines, Internet Relay Chat channels and e-mail can be important sources of threat information, as is the network traffic itself. A number of functions performed by public and private sector organizations depend upon access to and analysis of that information, including intelligence, evidence, and indications and warnings to name a few.

Intelligence is defined as information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. [2] The collection, analysis and reporting of timely, accurate intelligence on threats to national security is generally the responsibility of security and intelligence (S&I) agencies such as the National Security Agency (NSA) or the Central Intelligence Agency (CIA).[3] The intelligence function is no longer the exclusive domain of 'national security' agencies – private sector organizations need to generate competitive business intelligence. They may also receive intelligence from law enforcement and S&I agencies under the auspices of programs such as the FBI's Infragard)[4].

---

[2] From the Joint Doctrine Encyclopedia, dated 16 July 1997. Part of the US Department of Defense Joint Electronic Library.

[3] The CIA, for example, is mandated to "provide accurate, evidence-based, comprehensive and timely foreign intelligence related to national security". Extracted from "About the CIA: CIA Vision, Mission, and Values", posted to the CIA Website. See also: the Canadian Security Intelligence Service – "The Service shall collect and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected or constituting threats to the security of Canada", taken from (Canada (CA)) An Act to establish the Canadian Security Intelligence Service (R.S. 1985, c.C-23), updated to 31 August 2001 (*CSIS Act*), Section 12.

[4] Infragard was developed by FBI Cleveland in 1996 to promote protection of critical information systems. It provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities. Taken from the Infragard FAQ.

Intelligence includes identifying and monitoring groups or individuals deemed to pose a national security threat. Intelligence may be gathered in a number of ways, ranging from sophisticated technical means (e.g. satellites and signals intelligence efforts) to human intelligence sources (e.g. spies, defectors and informants). In order to fulfill their mandates, these agencies now undoubtedly include intercept and analysis (of both traffic and content) of open (i.e. public) information sources and network traffic as sources of intelligence about both conventional and cyber-based threat activity.[5]

Technological advances and the Internet provide expanded opportunities for criminal activity. As a result, law enforcement agencies face many new challenges, notably building the knowledge and skills necessary to effectively combat cyber crimes. Part of this knowledge may derive from an examination of open sources, including intercept and examination of network communications as a source of criminal intelligence. Interception activity is also undertaken to collect evidence of an (criminal) offense to support prosecution efforts.[6] The use of cyber-based evidence is becoming more important, and there is no reason to suppose that law enforcement agencies would not consider IDS logs as a potential source of cyber-based evidence.[7] While the collection of evidence to support criminal prosecution has traditionally been a law enforcement responsibility, S&I agencies are increasingly being tasked to support law enforcement in this regard, particularly in support of anti-terrorism efforts.[8]

Specific legislation exists to govern interception activities of S&I and law enforcement agencies. A number of conditions must be met before an interception authorization can be granted, and certain conditions must be also be met while conducting the interception. These conditions may be spelled out in the relevant

---

[5] European Parliament Report on the existence of a global system for the interception of private communications (ECHELON interception system) (2001/2098(INI)), report reference A5-0264/2001, dated 11 July 2001. The report refers to claims that ECHELON has 'the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents' (Section 1.6, page 23) while acknowledging that limitations on interception and analysis make this kind of global surveillance 'impossible in practice' (Preamble, page 11, Item D).

[6] Gellman, B., Washington Post Staff Reporter, "Cyber-Attacks by Al Qaeda Feared", dated 27 June 2002. In this case, FBI review of network audit and monitoring logs revealed that al Qaeda operatives were spending time on sites dealing with supervisory control and data acquisition (SCADA) systems – the systems that control power, water, transport and communications grids. See also: Pruitt, S., IDG News Service, "FBI gets new Web searching powers", dated 31 May 2002.

[7] While the admissibility of electronic records has been the subject of past case law, it is not clear if IDS logs have been included. For issues associated with the use of IDS logs as evidence, see: Sommers, P., "Intrusion Detection Systems as Evidence", First International Workshop on the Recent Advances in Intrusion Detection, 14 – 16 September 1998, Louvain-le-Neuve, Belgium; and Stephenson, P., "The Application of Intrusion Detection Systems in a Forensic Environment" (extended abstract), Third International Workshop on the Recent Advances in Intrusion Detection, 2 – 4 October 2000, Toulouse, France.

[8] See e.g.: (UK) An Act to give the Security Service the function of acting in support of the prevention and detection of serious crime, and for connected purposes (1996 Chapter 35), 18 July 1996 (*Security Service Act 1996*), Section 1(1).

governing legislation (e.g. CSIS Act) or other legislation (e.g. criminal or anti-terrorism law).[9]

Other public and private sector organizations also have a requirement to intercept and examine network traffic. While these organizations may need to do this for intelligence or evidentiary purposes, most such interception would likely be conducted by law enforcement or S&I agencies. Instead, interception performed by these organizations is more commonly done in order to identify an attempted or actual intrusion into a protected system or network, and to initiate an incident response process (of course, this also applies to law enforcement and S&I agencies). While existing legal regimes adequately address interception by S&I and law enforcement agencies, they generally do not adequately address interception of network traffic by other organizations.

4 What Is a Private Communication?

What constitutes a private communication, particularly those over a network, for the purposes of criminal or anti-terrorism law? The only definition of private communications that could be found in the selected legislation is that in the *Criminal Code of Canada*. A private communication is defined as "any oral communication or any telecommunication, … that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it."[10] Telecommunications is further defined as "the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system".[11] Network communications, although not explicitly mentioned anywhere in the legislation, would almost certainly fall within this definition. Note that it is the expectation of the

[9] See e.g. (AU) An Act to prohibit the interception of telecommunications except where authorized in special circumstances or for the purposes of tracing the location of callers in emergencies, and for related purposes, Act No. 114 of 1979 as amended (the Telecommunications (Interception) Act of 1979), Part III, Sections 9 – 11; (CA) *CSIS Act*, Section 21; (CA) An Act respecting the Criminal Law (R.S., C-34), updated to 31 August 2001 (*Criminal Code)*, Section 184.2(3); (UK) Regulation of Investigatory Powers Act 2000 (2000 Chapter 23), dated 28 July 2000 ((UK) RIPA 2000), Part I, Sections 6 – 11; (US) US Code, Title 18, Part I, Chapter 119, Section 2516 (Authorization for interception of wire, oral, or electronic communications (in criminal cases)); and (US) US Code, Title 50, Chapter 36, Subchapter I, Section 1804 (Applications for court orders (for Foreign Intelligence Surveillance Act interceptions)).

[10] (CA) *Criminal Code*, Section 183. Other legislation defines private communication services, but not private communication. See also: (UK) RIPA 2000, Part I, Section 2(1); (US) US Code, Title 26, Subtitle D, Chapter 33, Subchapter A, Section 4241 to 4243, Subchapter B, Section 4252(d).

[11] (CA) An Act respecting the interpretation of statutes and regulations, updated to 31 August 2001 (*Interpretation Act*), Section 35(1). The Interpretation Act provides the authoritative basis for the definition and interpretation of selected terms that appear in other Canadian legislation. See also: (AU) Telecommunications (Interception) Act 1979, Section 5(1); (US) US Code, Title 18, Part I, Chapter 119, Section 2510(14); and (UK) RIPA 2000, Part I, Section 2(1).

originatorof the message that no one other than the intended recipient will intercept the message that matters to the determination of whether the communications is a 'private communication'.

It might be useful at this point to try to distinguish between personal information that is public and that which is private[12]. Personal information is defined as information about an identifiable individual that is recorded in any form including any identifying number, symbol or other particular assigned to the individual, or the address of the individual.[13] Personal information has been construed as being very broad and probably includes Internet Protocol (IP) addresses. Some personal information should be considered private (e.g. financial or medical information). Some personal information, on the other hand, clearly resides in the public domain (e.g. name, street address and phone number in a phone book) and would likely not be considered private, although there are exceptions (e.g. unlisted phone number). In a network context, the equivalent information would be user name and domain (e-mail) and the corresponding addressing information as published, for instance, in a public key certificate. Although personal, this would likely constitute public information.

Is the issue one of keeping the content of a particular communication private? There is little argument that the user-entered portion of a communication would be considered personal and private. If the originator does not want the contents of the message to be read by anyone other than the intended recipient, then he/she can take steps to protect the message content through the use of encryption. In fact, criminal law specifically refers to electronic or other treatment of radio-based communication for the purpose of preventing intelligible reception by any person other than the intended recipient.[14] There is no mention of similar treatment for other forms of telecommunication (i.e. network communications). However, should an individual consciously take steps to protect the communication against intercept, given the generally inclusive definition of telecommunications, it is the author's opinion that a reasonable expectation of privacy would be created for the content of network communications.[15]

The situation is not quite so clear when it comes to packet header information. Are headers an integral part of the communication (i.e. part of the content of a message)?

---

[12] Public is defined as "open to or shared by all the public", or "reveal previously unknown information." Private is defined as "confidential; not to be disclosed to others", or as that which is "kept or removed from public knowledge or observation". The Canadian Oxford Dictionary, Oxford University Press, 1998.

[13] (CA) An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves (R.S. 1985, c.P-21), updated to 31 August 2001 (*Privacy Act*), Section 3. The identification of the individual may also include one or more factors relating to his physical, physiological, mental, economic, cultural or social identity and includes any expression of opinion about the individual.

[14] (CA) *Criminal Code*, section 183. See also: (US) US Code, Title 18, Part I, Chapter 119, Section 2510(16).

[15] However, provisions for the mandatory disclosure of encryption keys are being enacted into law. See e.g.: (UK) RIPA 2000, Part III, Section 50. In light of this, some authors are advocating measures intended to circumvent the provisions of this Act. See: Brown, I. and Gladman, B., "The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", undated.

An argument could be made in favour of this position as at least part of the header (e.g. the destination address in an e-mail, or the URL of a website) is generated in response to user input. Intuitively, one would consider this to be private information – individuals may not want anyone else to know with whom they are communicating. On the other hand, there is a certain amount of information in network communications that must be public. This, of course, is the routing and handling information contained in the packet header. If one considers conventional mail, the header information would be analogous to the addressing on the outside of an envelope. The majority of this information is generally available to the public (other than on the envelope itself, which is afforded some privacy by virtue of being handled within the postal system) and would therefore be considered public, not private, information.

Is the issue then one of keeping the fact that a particular communication has occurred private? Simply intercepting the fact of a communication (i.e. traffic data) can lead to the development of a detailed user profile (through traffic analysis) that could reveal personal, private information (e.g. web surfing habits) even if the data from which the profile is constructed is all considered to be public.[16] Traffic data is defined as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[17] In a telephone context, traffic data is generally considered to be a list of telephone numbers dialed to or from a specific telephone line. It is straightforward to separate the dialed number from the content of the telephone conversation.

In a network context, there is a difference of opinion as to what constitutes the equivalent of the dialed number list. The range of possibilities extends from the header (or addressing) portion of network traffic to the address and subject lines of an e-mail and Web URLs.[18] The only thing that seems to be consistent across the differing views is that traffic data will contain IP addresses. Given the nature of the information that can be logged by an IDS, it would almost certainly fall within the

---

[16] This will increasingly be an issue now that data retention legislation is being passed. See e.g.: (UK) An Act to amend the Terrorism Act 2000; …; to provide for the retention of communications data; …; and for connected purposes (2001 Chapter 24), 14 December 2001 (*Anti-terrorism, Crime and Security Act 2001*), part 11; and Reuters, "Spain passes law to regulate Internet content", dated 27 June 2002. This article makes mention of the Law on the Information Society and Electronic Commerce (LSSI), which includes provisions for ISPs to keep details on users for over a year.

[17] (Council of Europe(COE)) Convention on Cybercrime (ETS 185), opened for signature at Budapest, 23 November 2001, Chapter I, Article 1(d). "Origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. "Destination" refers to a comparable indication of a communications facility to which communications are transmitted (from Explanatory Memorandum to the Convention, article 30). See also: (US) US Code, Title 18, Part II, Chapter 206, Section 3127(3), as amended by the USA PATRIOT Act; and (UK) RIPA 2000, Part I, Section 2(9).

[18] Black, J., "Uncle Sam Needs Watching, Too", published in Business Week Online, 29 November 2001. See also: Weinstein, L. and Neumann, P.G., "PFIR Statement on Government Interception of Internet Data", published by People for Internet Responsibility (PFIR), dated 7 September 2000.

definitions of traffic data, which has potentially significant implications with respect to data retention. The difficulty comes in separating addressing information from content, given that both travel together in network packets. Even configuring IDS to log only the header portion of the packets does not adequately address this shortcoming – IDS must still 'intercept' the entire packet in order to scan it for indications of malicious traffic.

There seems to be, at least in certain legislation, a definite effort to distinguish between 'traffic' data and content. For example, the Council of Europe (COE) Convention on Cybercrime refers to interception and real-time access to traffic data.[19] United States Code (criminal law) contains provisions for the use of pen registers and trap and trace devices. These devices are capable of monitoring and identifying the specific phone numbers dialed from a particular telephone line - they do not capture or record the content of any such communication.[20] That certain legislation distinguishes between traffic data and content implies that traffic data is not considered to be private communications.[21]

If the originator wants to disguise the fact that they initiated a particular message (e.g. a web session), then he/she has the option of using pseudonymizing techniques. At the very least, the use of these techniques would increase the expectation on the part of the originator that his/her communication will be private, and therefore would be subject to the relevant provisions of criminal or anti-terrorism law. However, even this is not definitive as many of these techniques provide a mechanism for associating the pseudonymized communication with a particular individual in certain circumstances.[22] Even the use of anonymizing techniques might not be sufficient to address this issue – if the disclosure of encryption keys can be forced, could providers of anonymizing services be forced by law to retain sufficient records to re-associate anonymized traffic with the originator?

---

[19] (COE) Convention on Cybercrime (ETS 185), Title 5, Article 20. Article 21 deals separately with the interception of content data.

[20] (US) US Code, Title 18, Part II, Chapter 206, Sections 3127(3) and (4). Pen registers are devices that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. Trap and trace devices are devices which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted. See also: (US) An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes, dated 26 October 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001) (hereinafter USA PATRIOT Act). The USA PATRIOT Act amends US Code Title 18, Part II, Chapter 206, Section 3127(3) and (4) to refer to recording or decoding dialing, routing, addressing or signaling information, but not including the contents of such communication.

[21] Lee, S.C. and Shields, C., "Tracing the Source of Network Attack: A Technical, Legal and Societal Problem", published in the proceedings of the 2001 IEEE Workshop on Information Assurance and Security, pages 239 – 246. This is at least the case in the U.S. In their paper, the authors state "legally, there is no expectation of privacy for packet headers" (page 245).

[22] For a discussion of the use of pseudonymization techniques to enhance the expectation of privacy in network communications, see Johnston, Steven R., "The Impact of Recent Privacy and Data Protection Legislation on the Sharing of Intrusion Detection Information". In W. Lee, L. Me, A. Wespi (Eds.), Proceedings of Recent Advances in Intrusion Detection 2001 (RAID 2001), pgs. 150 – 171, Springer-Verlag, Berlin Heidelberg, 2001.

What expectation of privacy does an individual involved in malicious activity have – do they forfeit any expectation of privacy with respect to those activities? According to provisions in the USA PATRIOT Act, a computer trespasser is "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through or from the protected computer."[23] In any event, expectations of privacy are probably considerably different in each case. Whatever the expectations, IDS are not sufficiently discriminating to distinguish between malicious activity (which should be monitored and logged) and benign activity (the privacy of which should be respected).

If the above analysis is correct, then the header portions of communications over the Internet would probably not be considered private. This distinction may prove to be important when interpreting the legislation in particular, and in configuring IDS to conform to the law. What exactly are the relevant provisions of criminal and anti-terrorism? How do organizations use IDS in a lawful manner?

5 Criminal Law

Criminal law generally prohibits the intercept of private communications. For example, the *Criminal Code* states: "every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence".[24] Electro-magnetic, acoustic, mechanical or other device includes any device or apparatus that is used or is capable of being used to intercept a private communication.[25] Intercept includes "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof".[26]

It is important to note that an IDS is a computer in its own right, with a processor, primary and secondary storage, and input/output elements. The input element is the interface to the network, typically a network interface card (NIC) designed to IEEE 802.x standards. This interface operates in promiscuous mode, and it 'captures' every well-formed link-level frame – the format for the transmission of IP datagrams across a network. Once they have been 'captured' by the NIC, a copy of the frames and their contents (i.e. the information they contain) are placed in the sensor's primary memory for analysis. Even if the IP datagrams are eventually discarded (because they are deemed to be legitimate traffic), the IDS is in fact copying all of the network traffic.

---

[23] (US) USA PATRIOT Act of 2001, dated 26 October 2001, section 217. This section amends US Code, Title 18, Part I, Chapter 119, Section 2510 by adding a new subsection 2510(21) containing the definition of a computer trespasser. None of the other legislation contains a statement of this nature.

[24] (CA) *Criminal Code*, section 184(1). Similar offences exist under: (AU) The Telecommunications (Interception) Act 1979), Section 7(1); (US) US Code Title 18, Part I, Chapter 119, Section 2511(1); and (UK) RIPA 2000, Part I, Sections 1(1) and 1(2).

[25] (CA) *Criminal Code*, section 183. See also: (AU) Telecommunications (Interception) Act of 1979, Section 5(1); (US) US Code, Title 18, Part I, Chapter 119, Section 2510(5); and (UK) RIPA 2000, Part V, Section 81(1)

[26] (CA) *Criminal Code*, section 183. See also: (AU) Telecommunications (Interception) Act 1979, Section 6; (US) US Code Title 18, Part I, Chapter 119, Section 2510(4); and (UK) RIPA 2000, Part I, Section 2(2).

For the purposes of criminal law, is it essential that packet contents be intercepted, or does it still constitute an intercept if only the packet header is captured? Does the intercept take place when the link-level frame is copied into memory, or does it only take place when the packet is logged because it has been deemed to be malicious? These questions will probably only be answerable in a court of law. In the author's view, however, given that IDS make a copy of all network traffic, regardless of what they actually log, the use of IDS will almost certainly be considered to fall within the definition of device, and to be considered an intercept within the meaning of criminal law.

5.1 Exemptions in Criminal Law

The above analysis led to the conclusion that the use of IDS would likely, by strict definition, constitute an offence against relevant provisions in criminal law. There are, however, exemptions in the criminal law that specify conditions under which intercept would not be an offence. In general, the exemptions are where consent to the interception, express or implied, has been given by the originator of the private communication or the intended recipient; where an authorization has been obtained; and where the interception is by a person engaged in providing a telephone, telegraph or other communication service to the public.

Consent

Consent provisions imply that one party consent to the interception (i.e. either the originator or the intended recipient) is sufficient to exempt the individual performing the interception from the effects of criminal law. Obtaining the consent of the recipient (e.g. the employee) may be straightforward by making consent part of the conditions of being granted a network account, or use banners indicating that the information system being used is subject to being monitored for security purposes, and that continued use of the system constitutes consent to such monitoring.[27] What happens if an individual sends a communication to the wrong address? Does the (unintended) recipient have a right to consent to its interception? The answer to this question is not at all clear.

Obtaining the consent of originators (i.e. persons outside the organization where the monitoring is taking place) may be more problematic. Two key concepts related to consent are knowledge and choice. Does the individual know that the intercept is taking place? Ensuring that the originator knows the interception is taking place may be problematic. Does the individual have a realistic choice – is there an alternative communications path that is not subject to monitoring (intercept)? In terms of network communications, the answer to the latter question is probably no – most organizations will try to ensure that all points of interconnection to the Internet are adequately protected against intrusions (including the use of IDS).

[27] However, mere employee consent to surveillance is no longer sufficient to justify unlimited surveillance activities. Surveillance is to be limited to that which a reasonable person would consider appropriate. See: Geist, M., "Shift to more workplace privacy protection", dated 28 June 2002, Globe and Mail newspaper (online).

There is also the issue of implied consent. For an individual external to the organization, does the continued use of the computer system really constitute consent to monitoring for security purposes? Does the posting of a legal or privacy policy to a website create a diminished expectation of privacy? Should consent to intercept be implied by the simple act of sending an e-mail? In the absence of definitive proof that the individual initiating the communication knew that the communication would be subject to intercept, it is likely that the courts would tend to be conservative and deem that the originator has a reasonable expectation that the communication would not be intercepted.[28]

The Supreme Court of Canada has held that one party consent to the monitoring of private communications, even though it does not contravene the provisions of the *Criminal Code*, violates the protection provided by Section 8 of the *Charter*, dealing with search and seizure.[29] This implies that organizations could not rely on this provision to provide adequate legal authority to conduct intrusion detection.

Authorization

In order for an authorization for the interception of private communications to be granted under criminal law, there must be reasonable grounds to believe that an offence against criminal law has been or will be committed; either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and there must be reasonable grounds to believe that information concerning the offence will be obtained through the interception sought.[30] Authorizations are required for each instance of interception, and requests for authorization must specify the particulars of the offence. When the authorization is granted, it will specify the identities of the persons, if known, whose private communications are to be intercepted, and the period for which the authorization is required.[31] Most authorizations can only be granted for a maximum of 60 days before they need to be renewed.

Criminal law provisions for interception of private communications are not generally suited to interception of private communications for network protection. Given the unpredictable nature of network intrusions, it would be difficult to provide particulars of the offence that will be committed. In most cases it will be impossible to accurately identify the responsible individuals, and for intrusion detection purposes, the authorization would need to be permanent.

---

[28] Rubinkam, M., "Court to Decide on Web Wiretapping", Los Angeles Times article, dated 19 February 2002. In this article, the author refers to a case heard by the Pennsylvania Superior Court. The court ruled that the accused "had consented to the recording by the very act of sending e-mail and instant messages". The court further stated that "any reasonably intelligent person, savvy enough to be using the Internet… would be aware that messages are received in a recorded format, by their very nature". While not authoritative, a court in Canada may find this case informative/instructive.

[29] Insert relevant case law reference.

[30] (CA) *Criminal Code*, Section 184.2(3). See also: (AU) Telecommunications (Interception) Act of 1979, Sections 9 – 11; (US) US Code, Title 18, Part I, Chapter 119, Section 2518(3); and (UK) RIPA 2000, Part I, Sections 5(2) and 5(3).

[31] See e.g.: (CA) *Criminal Code*, Section 184.2(4).

Telecommunications Service Providers

Criminal law provides exemptions relating to interception of private communications by the provider of a telephone, telegraph or other communication service[32] to the public. The terms telephone and telegraph are not explicitly defined in criminal law, however, the definition of telecommunications is sufficiently broad that telephone and telegraph communication services would likely cover network services.

Interception must be necessary for the provision of the service, or it must relate to service observing or random monitoring for the purposes of service quality control checks. Depending on the service being provided, an argument could easily be made that the use of IDS as an integral component of a layered security architecture is essential to ensure the quality of the service, especially confidentiality, integrity and availability. Other methods of detecting intrusions, such as detailed review of all entries in device logs, are potentially more invasive than the use of IDS, which act as a filter to reduce the volume of information examined by an analyst.

These conditions, which would seem to apply to the use of IDS, apply to a person who is providing a telephone, telegraph or other communication service to the public. A key reason for public and private sector organizations moving online is to be able to improve the service they provide to the public. However, it is not at all clear if this is sufficient for them to be considered a telecommunications service provider for the purposes of criminal law. This is an issue that will require further analysis.

Previous analysis led to the conclusion that the header portions of network traffic probably do not constitute private communications. However, the use of IDS for network traffic monitoring would probably still constitute an intercept under criminal law, as the initial copying of network traffic includes content, even if it is not subsequently logged. An examination of existing criminal law exemptions suggests their application to public or private sector organizations would be problematic at best. They were intended for the intercept of private communications for the purposes of collecting evidence of a criminal offence, not for network protection purposes.

6 Anti-terrorism Law

Prior to September 11, the interception of private communications was governed by criminal law as discussed above. The general conclusion was that the use of IDS may constitute an interception as defined in criminal law, and that the existing exemptions did not adequately address the interception of private communications for network protection purposes. In response to the attacks on the World Trade Center and the Pentagon, a number of countries either initiated or accelerated plans to introduce

[32] See e.g.: (COE) Convention on Cybercrime (ETS 185), Section 1A, article 1(c), and Explanatory Report, article 26. “Service provider” means any public or private entity that provides to users of its service the ability to communicate by means of a computer system. The term "service provider" is deliberately broad, and may include a closed group or the facilities of a provider that are open to the public, whether free of charge or for a fee. The closed group can be, for example, the employees of a private enterprise to whom the service is offered by a corporate network.

comprehensive anti-terrorism legislation.[33] Not all of the bills were passed - Australia's Telecommunications Interception Amendment Bill 2002 (designed to give government agencies authority to read e-mail, SMS and voice messages without an interception warrant) was defeated in the Australian Senate.[34] Most of these bills were omnibus bills, meaning they introduced a variety of new measures, frequently by amending existing criminal law. Of these, the most controversial and of most relevance to intrusion detection are those dealing with interception of telecommunications and data retention.

6.1 Interception of Private Communication

Prior to the introduction of anti-terrorism legislation, the interception of private communications was conducted in accordance with strict rules. Specific conditions had to be met before an authorization could be granted, and strict conditions applied to the actual conduct of the interception. Interception was also generally limited to telephone communications. This tended to restrict the circumstances in which interception could be conducted. For instance, a wiretap order only applied to a single telephone number. There was some judicial discretion with respect to granting or denying requests for authorization. This combination provided a certain degree of assurance that the privacy of network communications would not be violated without cause.

In the wake of the September 11 attacks, there were calls to grant law enforcement agencies much broader powers to monitor private communications and access personal information. The bills generally responded to these calls by amending existing criminal law provisions governing interception of private communications. The nature of the information that can be captured has been broadened to include dialing, routing and addressing information, effectively enabling law enforcement agencies to monitor and intercept electronic mail, web surfing and other forms of electronic communications.[35] Law enforcement agencies are now permitted to obtain

---

[33] The US signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) into force on 26 October 2001. Canada's Bill C-36 (An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism (the Anti-Terrorism Act)) came into force 24 December 2001. The UK's Anti-terrorism, Crime and Security Act became law on 14 December 2001. See also: Hayes, Ben, "EU anti-terrorism action plan: legislative measures in justice and home affairs policy", Statewatch post 11.9.01 analyses: No. 6. See also EU Press Release "Action by the European Union following the attacks on 11 September", MEMO/01/327 dated 15 October 2001, available from RAPID - The Press and Communication Service of the European Commission.

[34] Fitzsimmons, C., "Email snooping bill knocked down", dated 28 June 2002, AustralianIT (online).

[35] (US) USA PATRIOT Act, Section 216(c)(2) and (3) amend the definitions of pen register and trap and trace device respectively to permit recording of dialing, routing and addressing information, although there are still restrictions on the recording of communications content. It is important to note that concerns surrounding interception of e-mail pre-date September 11 – witness the controversy surrounding the FBI's Carnivore (now DCS1000) program.

a single authorization to tap any communications that a suspect may use. Combined with claims that the level of judicial discretion has essentially been drastically reduced, this has prompted fears of the potential for massive invasions of privacy[36]. Whether these fears are justified or not, the amendments still do not provide a general authorization for interception of network communications by public and private sector organizations – they must still operate under the prior, more restrictive regime.

There appear, however, to be two exemptions to the above statement. The first comes in Canada's *Anti-Terrorism Act*. This Act includes a specific clause authorizing intercept of private communications for the purposes of protecting GoC computers and networks.[37] However, this clause only applies to a single government agency (CSE) and then only under strict conditions, similar to those in the *Criminal Code*.[38] An authorization made under this section may contain any conditions that the Minister considers advisable to protect the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications. There is at least an indication, therefore, that attempts will be made to respect the privacy of network communications.

It is important to remember, however, that this authorization can only be provided to CSE, leaving all other GoC departments and agencies without a specific legislative basis for the conduct of intrusion detection. Provision does exist within the act for persons who assist with the execution of the authorization to be covered by the authorization[39], but the implications of this for the GoC, from an operational perspective, have yet to be examined.

The second exception is a provision in the USA PATRIOT Act, which amends US Code to add a provision that "it shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; and such interception does not acquire communications other than those transmitted to or from the computer trespasser.''[40]

At first glance, this would appear to provide, in the United States at least, owners of a protected computer[41] the legal right to intercept private communications.

---

[36] See: Anonymous, "How the USA PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance", dated 23 October 2001. See also: Anonymous, "Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information", dated 24 September 2001.

[37] (CA) *Anti-Terrorism Act*, Part 5, clause 273.65(3). The Minister (of National Defence) may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, …..„authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization. This clause was developed specifically with the use of IDS in mind.

[38] (CA) *Anti-Terrorism Act*, Part 5, clause 273.65(4).

[39] (CA) *Anti-Terrorism Act*, Part 5, clause 273.67.

[40] (US) USA PATRIOT Act, article 217, amending US Code, Title 18, Chapter 119, Section 2511(2).

[41] (US) US Code, Title 18, Part I, Chapter 47, Section 1030(e)(2).

However, it may not be as simple as that. First, the definition of protected computer appears to be fairly narrow, being a computer that is exclusively for the use of a financial institution or the United States Government or which is used in interstate or foreign commerce or communication. In relation to the private sector, for instance, what computers would this cover – individual workstations, web or mail servers (which could arguably be for foreign communication)? The answer to this question is not at all clear.

Second, the interception must only acquire the communications of the computer trespasser. Whether the term 'acquire' refers to the logging of specific communications, or to the copying of communications performed by an IDS prior to scanning, IDS are not sufficiently discriminating to ensure that only communications from the computer trespasser will be 'acquired'. There does not appear to be any issue with the IDS sensor scanning network traffic looking for indications of malicious activity and generating alerts/alarms as a result of the scanning. The problems appear to arise when a human analyst must examine any flagged traffic to validate the alarm (i.e. is it a valid alarm, or a false positive?). Even if they only log traffic deemed to be malicious, the current state IDS technology almost guarantees that at least some of this traffic will be benign (i.e. false positives), thereby violating this condition. In the absence of judicial interpretation of this provision, it is unlikely that organizations could generally rely upon it for legal authority to intercept private communications.

6.2 Data Retention

The second controversial provision in most anti-terrorism law concerns data retention.[42] A distinction must be made between data preservation, where data is stored and retained in response to a specific request and data retention, where the data is stored as a routine practice. As a general rule, there seems to be very little controversy associated with data preservation. On the other hand, data retention is causing a great deal of concern, especially among ISPs. Prior to the introduction of the anti-terrorism legislation, traffic data was only retained as long as was necessary for billing purposes, and at the end of that period was either to be anonymized or destroyed. Combined with the increasing trend to billing flat rates for network access, this ensured that a minimum of private information was collected and stored.

The anti-terrorism legislation not only increased the duration for which this information had to be stored, it also considerably expanded the information to be retained[43], although it appears as if it is predominantly traffic data that is to be

[42] Provisions for data retention are also found elsewhere. See e.g.: Anonymous, "Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronics communications sector", document reference /*COM/2000/0385 final – COD 2000/0189*/ (replacing Directive 97/66/EC, adopted 15 December 1997). This proposal was accepted in a vote in the European Parliament 30 May 2002.

[43] Anonymous, "List of Minimum and Optional Data to be Retained by Service Providers and Telcos", Expert Meeting on Cybercrime: Data Retention, The Hague, 28 December 2001 (File No. 5121-20020411LR-Questionnaire). The list of information to be retained is quite extensive: user-id and password (remote login); sender and receiver (login@domain), identifying information of e-mail retrieved (e-mail); and hostname or IP address, nickname used during session (IRC).

retained. While this was aimed at e-mails and web traffic, there is no reason to suppose that data collected by IDS would not be covered by these provisions, as it likely falls within the definition of traffic data. While this poses a number of data storage and management problems, it also poses problems with respect to privacy of network communications. As mentioned, IDS are prone to generating false positives. Unless procedures are in place to examine all of the flagged traffic, and then to destroy that which is determined to be benign, examination of the logged data will almost certainly result in privacy violations. Even if the data is anonymized, it is likely that law enforcement agencies would require its association with a particular originator for investigative purposes (if provisions exist to force disclosure of encryption keys, then requiring this association is likely to follow).

7 Conclusions

This paper has looked at some of the issues that will need to be addressed in order to develop a general legal framework for use of IDS, including trying to define what is meant by a 'private communication'. Depending on the nature of the communication, the originator might want to hide the content of the communication (through cryptography), the fact that a communication has taken place (through anonymization or pseudonymization) or both. The use of encryption to ensure the privacy of the contents of a communication is no longer an assurance that the contents will in fact remain private – legislation exists to force the disclosure of encryption keys. Similarly, the use of pseudonymizing techniques is no guarantee that the fact of a communication will remain private – most schemes permit the re-association of the pseudonymized traffic with the originator. An attempt to legislate the creation and retention of similar records by providers of anonymizing services is not beyond possibility. If law enforcement agencies decide that IDS data is essential to their investigation, there is little reason to believe that they will not require this reassociation.

IDS log data probably falls within the definition of traffic data, and is, therefore, probably subject to the provisions of legislation that require the long-term retention of traffic data by service providers. If this is the case, this poses numerous challenges for the service providers, and creates an increased risk of privacy violations.

Based on the definitions found in criminal law and supporting legislation, the use of IDS by public and private sector organizations will likely constitute an intercept. In order not to be an offense, the use of IDS must be in accordance with one of the exemptions, namely where consent to the interception, express or implied, has been given by the originator of the private communication or the intended recipient; where an authorization has been obtained; or where the interception is by a person engaged in providing a telephone, telegraph or other communication service to the public.

These provisions do not adequately address the situation facing public and private sector organizations. Single party (i.e. recipient) consent, although lawful, has been held to violate constitutional law. Two party consent is considered the minimum standard – something that will not be achieved if one of the parties to the communication has malicious intent. While satisfying the conditions necessary to the granting of an authorization should generally be possible, authorizations issued under criminal law are for evidence collection, not network protection. It is unlikely that a global, open-ended authorization for network protection would (or could) ever be

granted under criminal law or withstand legal challenge. Narrower authorizations issued under the *Anti-Terrorism Act* (Canada) or to law enforcement or S&I agencies to intercept private communications for network protection (i.e. conduct intrusion detection) would be more likely to withstand challenge.

In a limited sense, a case could be made for the application of the criminal law exemption for telecommunications services providers to public and private sector organizations. However, it is not at all clear whether or not these organizations would actually qualify as a telecommunications service provider under criminal law and so organizations could probably not rely on this exemption. Anti-terrorism legislation greatly complicates the task of protecting the privacy of network communications and the personal information that they contain. Not only can a broader range of information be intercepted under authorization, but a similarly broad range of information is to be retained by ISPs and telephone companies. In addition, there appears to have been a reduction in the level of judicial discretion in the granting or denying of interception requests.

It is, therefore, reasonable to suggest that the key to addressing these deficiencies is the creation of a new exemption under criminal law. This exemption would provide the necessary legal basis for the interception of private communications for the purpose of protecting public and private sector computer systems or networks from mischief, unauthorized use or interference.

There is still a great deal of work that needs to be done to develop a general legal framework for the conduct of intrusion detection within the public and private sectors. Once the legal framework has been developed, additional work will be required in order to develop appropriate policies, standards and procedures for the use of IDS, especially with respect to what can be collected, how that information is to be handled, stored or disposed of and who has access to the information and under what circumstances. The assistance of the legal community would be invaluable in this endeavour.

References

[1] Anonymous, “About the CIA”, undated. URL: http://www.cia.gov/cia/information/info.html (25 June 2002)

[2] Anonymous, “Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information”, 24 September 2001, Electronic Privacy Information Center (EPIC). URL: http://www.epic.org/privacy/terrorism/ata_analysis.html

[3] Anonymous, “Critical Foundations: Protecting America’s Infrastructures”, The President’s Commission on Critical Infrastructure Protection, October 1997, Critical Infrastructure Assurance Office. URL: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

[4] Anonymous, “How the USA-PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance”, 23 October 2001, American Civil Liberties Union. URL: http://www.aclu.org/congress/1102301g.html

[5] Anonymous, Infragard Frequently Asked Questions. URL: http://www.infragard.net/faq.htm

[6] Anonymous, "List of Minimum and Optional Data to be Retained by Service Providers and Telcos", Expert Meeting on Cybercrime: Data Retention, The Hague, 28 December 2001 (File No. 5121-20020411LR-Questionnaire). URL: http://www.statewatch.org/news/2002/may/europol.pdf

[7] Anonymous, "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001.2098 (INI)), dated 11 July 2001, presented to the European Parliament. URL (Federation of American Scientists): http://www.fas.org/irp/program/process/rapport_echelon_en.pdf

[8] (Australia) "An Act to prohibit the interception of telecommunications except where authorized in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes", (the Telecommunications (Interception) Act 1979), Act No. 114 of 1979 as amended. This compilation was prepared on 7 January 2002 taking into account amendments up to Act No. 166 of 2001. URL: http://scaleplus.law.gov.au/html/pasteact/0/464/pdf/TeleInt79.pdf.

[9] Black, J., "Uncle Sam Needs Watching, Too", published in Business Week Online, 29 November 2001. URL: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011129_3806.htm.

[10] Brown, I. And Gladman, B., "The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", undated. URL: http://www.fipr.org/rip/RIPcountermeasures.htm

[11] (Canada) An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act, and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism, 24 December 2001 (*The Anti-Terrorism Act*). URL: www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_4/C-36_cover-E.html.

[12] (Canada) An Act respecting the Criminal Law (R.S., c.C-46), updated to 31 August 2001 (*The Criminal Code*). URL (Department of Justice Canada) http://laws.justice.gc.ca/en/C-46/index.html.

[13] (Canada) An Act respecting the interpretation of statutes and regulations, (R.S. 1985, c.I-21), updated to 31 August 2001 (*The Interpretation Act*). URL (Department of Justice Canada): http://laws.justice.gc.ca/en/I-21/index.html.

[14] (Canada) An Act to establish the Canadian Security Intelligence Service (R.S., C-23), updated to 31 August 2001 (the *Canadian Security Intelligence Service Act*). URL (Department of Justice Canada): http://laws.justice.gc.ca/en/C-23/index.html

[15] (Canada) An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves (R.S. 1985, c.P-21), updated to 31 August 2001 (the *Privacy Act*). URL (Department of Justice Canada): http://laws.justice.gc.ca/en/P-21/index.html

[16] Canadian Oxford Dictionary, Oxford University Press, 1998.

[17] (Council of Europe) Convention on Cybercrime (ETS 185), opened for signature at Budapest, 23 November 2001. URL: http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

[18] (Council of Europe) Explanatory Memorandum to Convention on Cybercrime, dated 8 November 2001. URL: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[19] Data Protection Working Party, "Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385", dated 2 November2000. URL: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp36en.pdf.

[20] (European Parliament) Anonymous, “Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronics communications sector”, document reference /*COM/2000/0385 final – COD 2000/ 0189*/. URL: http://europa.eu.int/eur-lex/en/com/pdf/2000/en_500PC0385.pdf

[21] EU Press Release “Action by the European Union following the attacks on 11 September”, MEMO/01/327 dated 15 October 2001. URL (RAPID - The Press and Communication Service of the European Commission): http://europa.eu.int/rapid/start/welcome.htm.

[22] Geist, M., “Shift to more workplace privacy protection”, dated 28 June 2002, Globe and Mail newspaper (online version). URL: http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20020628/EBGEISY

[23] Gellman, B., Washington Post staff writer, “Cyber Attacks by Al Qaeda Feared”, 27 June 2002, Washington Post (online version). URL: http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html

[24] Hayes, Ben, “EU anti-terrorism action plan: legislative measures in justice and home affairs policy”, Statewatch post 11.9.01 analyses: No. 6: URL: http://www.statewatch.org/news/2001/oct/analy6.pdf.

[25] Johnston, Steven R., “The Impact of Recent Privacy and Data Protection Legislation on the Sharing of Intrusion Detection Information”. In W. Lee, L. Me, A. Wespi (Eds.), Proceedings of Recent Advances in Intrusion Detection 2001 (RAID 2001), pgs. 150 – 171, Springer-Verlag, Berlin Heidelberg, 2001.

[26] Joint Doctrine Encyclopedia, dated 16 July 1997. US Department of Defense Joint Electronic Library. URL: http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

[27] Lee, S.C. and Shields, C., “Tracing the Source of Network Attack: A Technical, Legal and Societal Problem”, published in the proceedings of the 2001 IEEE Man, Systems and Cybernetics Information Assurance Workshop, pages 239 – 246. URL: http://www.ai.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW1C1(09).pdf.

[28] Pruitt, S., IDG News Service, “FBI gets new Web searching powers”, dated 31 May 2002, Computerworld Magazine (online version). URL: http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,71599,00.html

[29] Reuters, “Spain passes law to regulate Internet content”, dated 27 June 2002. Posted to SiliconValley.com. URL: http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3556967.htm

[30] Sommers, P., “Intrusion Detection Systems as Evidence”, as presented at the First International Workshop on the Recent Advances in Intrusion Detection, 14 – 16 September 1998, Louvain-le-Neuve, Belgium. URL: http://www.raid-symposium.org/raid98/Prog_RAID98/Full_Papers/Sommer_text.pdf.

[31] Stephenson, P., “The Application of Intrusion Detection Systems in a Forensic Environment”, extended abstract, as presented at the Third International Workshop on the Recent Advances in Intrusion Detection, 2 – 4 October 2000, Toulouse, France. URL: http://www.raid-symposium.org/raid2000/Materials/Abstracts/47/47.pdf.

[32] (United Kingdom) Regulation of Investigatory Powers Act 2000, Chapter 23, 28 July 2000. URL: http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm

[33] (UK) An Act to give the Security Service the function of acting in support of the prevention and detection of serious crime, and for connected purpose (1996 Chapter 35), dated 18 July 1996 (the *Security Service Act 1996*). URL: http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm

[34] (UK) An Act to amend the Terrorism Act 2000; to make further provision about terrorism and security; to provide for the freezing of assets; to make provision about immigration and asylum; to amend or extend the criminal law and powers for preventing crime and enforcing that law; to make provision about the control of pathogens and toxins; to provide for the retention of communications data; to provide for implementation of Title VI of the Treaty on Eurpean Union; and for connected purposes (2001 Chapter 24), 14 December 2001 (the *Anti-terrorism, Crime and Security Act 2001*). URL: http://www.legislation.hmso.gov.uk/acts/acts2001/10024—a.htm

[35] (United States) United States Code Collection, Legal Information Institute, Cornell Law School. URL: http://www4.law.cornell.edu/uscode/.

[36] (United States) An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes, dated 26 October 2001, (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001). URL: http://www.epic.org/privacy/terrorism/hr3162.pdf.

[37] (United States) United States Supreme Court, Record of Opinion, "Katz v. United States, 389 US 347 (1967)", decided 18 December 1967. Summary of opinion available at FindLaw http://findlaw.com/US/389/347.html.

[38] Weinstein, L. and Neumann, P.G., "PFIR Statement on Government Interception of Internet Data", published by People for Internet Responsibility (PFIR), dated 7 September 2000, available at http://www.pfir.org/statements/interception.