

Surveillance systems

Going for the throat: Carnivore in an ECHELON world - Part II

Talitha Nabbali, Graduate 2002, University of Western Ontario &
Mark Perry,¹ University of Western Ontario

Carnivore is a surveillance technology, a software program housed in a computer unit, which is installed by properly authorized FBI agents on a particular Internet Service Provider's (ISP) network. The Carnivore software system is used together with a tap on the ISP's network to "intercept, filter, seize and decipher digital communications on the Internet". The system is described as a "specialized network analyzer" that works by "sniffing" a network and copying and storing a warranted subset of its traffic. In the FBI's own words "Carnivore chews on all data on the network, but it only actually eats the information authorized by a court order". This article, in two parts, provides an overview of the FBI's Carnivore electronic surveillance system.

A. Carnivore and American law

There are many laws in the United States that make pen-register, trap-and-trace and wiretap surveillance legal. Yet, none of these laws specifically address electronic surveillance using IP sniffers such as Carnivore. Nonetheless, the FBI and the government maintain that the laws allowing for telephone surveillance can be applied to Carnivore and other such surveillance devices. The FBI and the US government maintain that Internet surveillance is analogous to telephone surveillance for which most of the laws concerning wiretapping were formulated.

The analogy between the telephone and the Internet is important in regards to the different set of laws applicable to Carnivore's two operating modes; pen mode and full content mode. The difference between Carnivore's two modes of operation is that pen mode allows the FBI to intercept origin and destination information (the envelope of the e-mail) as well as URLs of sites visited, whereas full-content mode allows the FBI to collect substantive data in addition to transactional information. By using the telephone analogy the FBI claims that they need not demonstrate probable cause when using Carnivore in pen-mode, since Carnivore should be subject to the same minimal legal restraints as pen registers used to record a telephone subscriber's outgoing calls and trap-and-trace devices that record incoming telephone

numbers for a particular subscriber.² Meanwhile, as with wiretaps on telephones, the FBI agrees that a higher legal threshold is needed to obtain a warrant for use of Carnivore in full-content mode.

This section will provide an overview of the laws that allow for Carnivore given that we accept that the Internet is sufficiently analogous to the telephone system for the purposes of wiretapping and investigation laws.³

The Omnibus Crime Control and Safe Streets Act governs the electronic interception of wire and oral communications. It places a higher burden on real time interceptions of oral, wire and electronic communications than the Fourth Amendment requires.⁴ In accordance with this Act, only judges can authorize applications for wiretaps. In order to obtain an authorization for a wiretap, law enforcement officials must demonstrate probable cause that a crime has been committed or is about to be committed, that normal investigative procedures have been tried and have not been sufficient and that the intercepted communications will most probably be relevant to the investigation.⁵

Title III mandates that a wiretap order must contain:⁶

- The identity of the person to be surveyed;
- The nature of the communications to be intercepted;
- The location of the facility where the court order to intercept is granted;
- A description of the type of communications to be intercepted;
- A statement of the particular offense to which these communications relate;
- The identity of the law enforcement agency authorized to intercept the communications;
- The period of time for which the interception is authorized;
- Whether the surveillance will be terminated as soon as communications related to the offense are obtained

In addition, Title III states that the interception of communications must be minimized, such that no additional communications other than those that the court order allows shall be captured or

recorded.⁷ For example, in the case of telephone surveillance, if the child of a suspect calls a friend, surveillance must be terminated for the call.⁸ Not only can the call of the child not be recorded, but law enforcement agents are not even allowed to listen to the call. Title III also demands, that within 90 days of the termination of the investigation, all targets and other parties whose communications were captured are notified of interception.⁹

Although, Title III of the Omnibus Crime Control and Safe Streets Act mandates that a court order must be awarded before any surveillance is to take place, there are exceptions, namely in cases where national security is compromised or there is an immediate danger of death or serious injury. However, even in such cases, interception can only proceed if a court order is given within 48 hours of the start of surveillance.¹⁰

Even though Title III imposes many regulations for full wiretaps, the restrictions on pen registers and trap-and-trace devices are far less stringent. Law enforcement agencies are not required to demonstrate probable cause when using either a pen register or a trap-and-trace device¹¹ since in accordance with Title III the use of either pen registers or trap-and-trace devices does not constitute a search under the Fourth Amendment.¹²

The Electronic Communications Privacy Act amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to create statutory legal protection for all types of wire and electronic communications content, including, but not limited to, computer and Internet based communications.¹³ Furthermore, ECPA clarified the difference between the obtainment of wiretap orders and pen-register and trap-and-trace orders by declaring that to wiretap communications “an agency must obtain a warrant based upon probable cause”, but to obtain a pen-trap order “an agent must merely certify that the information likely to be obtained is relevant to an ongoing criminal investigation.”¹⁴

The rationale behind the difference in obtaining these court orders is that, according to the Supreme Court of the United States’ 1979 decision in **Smith**¹⁵ there is no expectation of privacy in telephone numbers dialed in and numbers received.¹⁶ Therefore transactional information (addressing, routing, billing and other information generated by service providers) is not to be awarded the same level of protection as substantive data.

The Communications Assistance for Law Enforcement Agencies Act 1994 (CALEA)¹⁷

requires phone companies to possess the infrastructure to support surveillance tools such as pen register and trap-and-trace devices. More specifically, CALEA requires that all companies providing telecommunication services to the US install remote control ports on their routes that allow law enforcement agencies to easily extract any conversation in its entirety, up to 1% of the hub’s total traffic simultaneously.¹⁸ The installation of the remote control ports was to be done by 1998, unless a waiver was issued to extend implementation to October 24, 2000.

The FBI sometimes names CALEA as proof that their use of Carnivore is legal. Yet, the United States Court of Appeals for the District of Columbia Circuit noted in **United States Telecom Association**¹⁹ that “Because Congress intended CALEA to “preserve the status quo,” the Act does not alter the existing legal framework for obtaining wiretap and pen register authorization”, “providing law enforcement no more and no less access to information than it had in the past.”. CALEA does not cover “information services” such as e-mail and internet access.”²⁰

The 21st Century Department of Justice Appropriations Act²¹ passed in the House of Representatives on July 23, 2000, requires the FBI to provide an annual report to Congress detailing exactly how, when, where and why Carnivore has been deployed during the previous year. The Act was passed because Congress recognized that the FBI’s Carnivore surveillance system posed a potential threat to individual privacy.²² Section 306 of the Act demands that the annual report provided by the FBI detail:

- The number of times Carnivore has been deployed;
- The officials who approved of each use;
- The criteria used to approve the deployment request;
- The process used to submit, review and approve the request;
- The facilities where Carnivore boxes were placed;
- The information gathered during each deployment.

Both the Combating Terrorism Act of 2001 and the USA Patriot Act of 2001 were approved by the Senate in the wake of the terrorism attacks of September 11, 2001.²³ Both Acts enhance police wiretapping to more situations and make it easier for the FBI to deploy Carnivore.²⁴ With the implementation of these acts, any US or State

The FBI sometimes names CALEA as proof that their use of Carnivore is legal

Attorney General can give a court order for the installation of a Carnivore box, whereas previously only a judge could order such warrants.²⁵ Although it is possible to get a court order allowing for the interception of Internet transmissions from a US or State Attorney General, surveillance with such orders are limited to pen-mode collection.²⁶ In order to intercept substantive data the FBI must still seek a court order from a judge. The Combating Terrorism Act and the USA Patriot Act also extend circumstances where interception can begin without a court order to include “safety or attacks on the integrity or availability of a protected computer”, making computer hacking offenses comparable to threats to national security, public health and crimes that cause death and serious injury.²⁷

B. Other electronic surveillance

In order to make surveillance easier and to provide a salve to public unease concerning criminal activity on the Internet, many countries have passed legislation to make surveillance easier and more comprehensive. Most of these newly established legislations attempt to extend the interception capabilities that law enforcement agencies have over telephone communications (circuit switched networks) to Internet communications (packet switched networks), and make interesting comparisons to the US approach with Carnivore and supporting legislation. Following is an overview of the laws and policies regarding electronic surveillance around the world.

The United Kingdom’s Regulation of Investigatory Powers Act 2000 (RIPA), which received royal ascent on July 28, 2000,²⁸ is one of the most controversial surveillance laws in the world. RIPA has been deemed “the most pernicious invasion of privacy ever imposed by a modern democratic state”,²⁹ and has been criticized as violating the European Convention on Human Rights. The Act is composed of five parts, which include provisions for listening to mobile and satellite phone calls, intercepting pager messages and bugging switchboards.³⁰ However, the most controversial provisions are those concerning Internet surveillance. The legislative act forces all ISPs in the United Kingdom to install black boxes on their network to monitor all data as it passes and subsequently feed it to a central processing location controlled by the United Kingdom’s security service MI-5. Moreover, the Act contains provisions for government access to encryption keys (“GAK”).

The RIPA applies to “any system which exists (wholly or partly) in the United Kingdom”.³¹ Thus, everything sent to or through Britain is subject to surveillance, under the law. Considering the nature of Internet packet routing, this means that any packet could travel through Britain’s communication infrastructure and thus be surveyed by British intelligence. In order for surveillance of all Internet traffic to be possible, RIPA compels ISPs to install ‘black boxes’ that, when activated, send intercepted communications directly to MI-5’s new central monitoring station, the Government Technical Assistance Centre (GTAC) located inside MI-5’s London Headquarters. Controversially, RIPA specifies that requests for traffic data, e.g. web sites accessed, intended recipients of sent and received e-mails and logon transactions, do not require a warrant because such information is “purely statistical”³² and therefore can be requested by any governmental department in the interest of detecting crime.³³ In other words, RIPA allows for the mass surveillance of internet activities without judicial warrant or adequate oversight. Consequently, the act increases the power of public authorities without correspondingly increasing the scope of their oversight or their accountability.³⁴

However, like in American Law, under RIPA the content of communications can only be intercepted with a court order, although the reasons for a warrant are broad:³⁵

(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary--

- (a) in the interests of national security;*
- (b) for the purpose of preventing or detecting serious crime;*
- (c) for the purpose of safeguarding the economic well-being of the United Kingdom; or*
- (d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.*

Although RIPA demands that a court order for interception be obtained, it makes it a criminal offense to reveal to anyone that they are being surveyed or have been surveyed. According to RIPA, the revelation of the content, details or the existence of a surveillance warrant past or present bears a penalty of up to five years in jail.³⁶ Consequently, because the existence of surveillance

warrants are to be kept secret indefinitely, the British public will never be aware of the scope of MI-5's electronic surveillance.³⁷

Although the power granted by the Regulatory Investigatory Powers Act of 2000 to law enforcement officials in regards to electronic surveillance is very broad, it is the fact that RIPA contains provisions for government access to encryption keys (GAK) that has generated the most controversy. With the royal ascent of RIPA, the UK joins Malaysia, Singapore and India as the only countries in the world to pass key seizure legislation.³⁸ Under RIPA, encryption keys of individuals, users and companies can be warranted for the purpose of any type of investigation for which a warrant would be issued.³⁹ Lack of cooperation in regards to the handing over of encryption keys can result in a prison sentence of two years. Furthermore, as with warrants to intercept communications content, there is a silence imposed on the recipient of an encryption key disclosure order. However, it is questionable whether RIPA's GAK provision will be effective to deter crime. After all, criminals who are careful and clever in their use of computers and the Internet are capable of avoiding surveillance,⁴⁰ while criminals who are caught and forced to hand over their cryptographic keys would rather claim they lost their key and endure a maximum of two years in prison than hand over a key which could produce damning evidence of more heinous crimes.⁴¹

Opponents of RIPA allege that the Act's GAK provision breaches the European Convention on Human Rights Act 1998, which demands that legislation within all countries of the European Union meet several requirements, such as respect for private life and the right to a fair trial.⁴² The argument is made that under RIPA the right to a fair trial is impossible since the Act demands that Internet users provide encryption keys on pain of imprisonment, that is, the Act forces Internet users to incriminate themselves.⁴³ As there is a general right against self-incrimination, which forbids government officials from compelling a person to testify against herself, RIPA contravenes basic human rights. RIPA also breaches article 6 of the Human Rights Act of 1998, which states that the burden of proof cannot be reversed such that a suspect needs to provide the requested evidence to prove his innocence,⁴⁴ since RIPA puts the onus on Internet users to prove that they do not have a requested key or they have lost it.⁴⁵ Given its problems with human rights, RIPA would without a doubt be deemed unlawful if the

United Kingdom legislation was subject to such restraints.⁴⁶ RIPA cannot be revoked by a legal decision in the UK as constitutional challenges of this nature are not possible. Nonetheless, it is expected that RIPA will be challenged in the European Court of Human Rights.

Not only is RIPA's violation of human rights disconcerting, but its negative economic impact on the United Kingdom is also alarming. According to a report commission by the British Chambers of Commerce on the Bill, RIPA's:

*effect is likely to be a loss of confidence in e-commerce, unacceptable costs to business, and to the UK economy, confusion and uncertainty at numerous levels of business and an onerous imposition of the rights of individuals.*⁴⁷

The report claims that the cost of compliance to RIPA for British ISPs will be £640 million over the next five years and the loss and leakage to the UK economy will be about £46 billion in RIPA's first five years of implementation.⁴⁸ Furthermore, RIPA's key seizure provision creates many business risks including increased opportunity for industrial espionage, reduced trust and confidence in company security and market disadvantage in the global marketplace.⁴⁹ Many believe that investors and e-commerce will only return to the United Kingdom, when all countries impose such oppressive restrictions on Internet users.⁵⁰

It can be argued that not only does RIPA seem to metamorphosis the United Kingdom from a modern democratic state into a surveillance nation, it also seems to hold potential problems for the economy, whose Labour government had aimed to make it the most e-friendly state in Europe by 2002.⁵¹ Ironically, RIPA undermines the privacy and security of honest citizens and businesses, yet is most probably ineffective against criminals who are careful and sophisticated in their use of computers and the Internet.

On July 10, 2000, Ireland passed the Electronic Commerce Act of 2000⁵² which the Irish government believes will help Ireland become a hub for e-commerce.⁵³ The Act guarantees that Internet users within Ireland shall enjoy high levels of privacy by making it an offense for anyone, including law enforcement officials, to attempt to access the content of encrypted communications without authorization.⁵⁴ Although the Act provides extensive protection for encrypted communications, it does not prevent law enforcement officials from intercepting unencrypted communications, which is

RIPA undermines the privacy and security of honest citizens

allowed under Ireland's Interception of Telecommunications Act of 1993.⁵⁵

Russia's *Sistema Operativno-Rozysknykh Meropriyati*, known in English as Russia's System of Operative Investigative Procedures or System of Ensuring Investigative Activity was introduced in two parts. The first part, SORM-1, came into affect in 1994 and gave the FSB, Russia's internal counterintelligence service (formerly known as the KGB), the right to monitor all telecommunications transmissions provided they first obtained a court order.⁵⁶ The second phase of the SORM legislation, SORM-2, came into affect in July 1998,⁵⁷ and requires that all ISPs install black boxes that provide a secure link between their ISP and the FSB's Data Collection Center (DCC)⁵⁸ such that the DCC can capture Internet transmissions within seconds.⁵⁹

In many respects, SORM is very similar to the United Kingdom's Regulation of Investigatory Powers Act (RIPA) since both legislative acts allow for the widespread surveillance of Internet communications within their respective jurisdictions.⁶⁰ However, although the United Kingdom is considered far more democratic than Russia, it seems that the abolishment of SORM is more probable than the revoking of RIPA. SORM has never been passed in Russian Parliament and as it stands contravenes article 23 of the Russian Constitution, which guarantees a right to secrecy of communications.⁶¹ Therefore, through legal challenges SORM can be revoked or altered.

Through Russia's democratic appellate process SORM has already been altered. In 2000, SORM was challenged in the Supreme Court of Russia by an appeal filed by a St. Petersburg journalist named Pavel Netupsky.⁶² The result of this appeal was that the Supreme Court of Russia nullified article number 130 of the Ministry of Communications Order, which allowed the FSB to survey electronic communications without informing ISPs of the reason or the target of their surveillance.⁶³ After having abolished article 130 of the Ministry of Communications Order, electronic surveillance can now only be conducted if a court order, specifying the reasons for surveillance, is presented to an ISP.⁶⁴ It is important to note that although ISPs will know the identity of the person or persons being surveyed, this does not mean that the target of an investigation will be notified that they have been surveyed or are being surveyed. Therefore, although SORM has been altered, it still seems to contravene article 23 of the Russian Constitution. Consequently, it is evident that only through multiple legislative amendments

will SORM possibly become constitutional.

Nonetheless, following the crisis of Chechen guerrillas taking theatregoers hostage in October 2002, there were many reports of Russian cell phone users seeing that their encryption services were no longer functional, believed to be removed to allow for SORM wiretapping of cell communications.⁶⁵

On August 13 1999, the Diet, the Japanese legislative assembly, passed the Communications Interception Law, modeled after the 1994 American Communications Assistance for Law Enforcement Agencies Act (CALEA), which allows law enforcement agencies to wiretap telephone, fax and internet communications.⁶⁶ It has been rumored that Japan was pressured into creating such a law by the United States government.⁶⁷ Prior to passing of the Communications Interception Law, wiretapping was illegal in Japan because it was said to violate article 21 of Japan's constitution and was explicitly prohibited under article 104 of Japan's Telecommunications Business Law and article 14 of Japan's Wire Telecommunications Law.⁶⁸

The Japanese Wiretapping Act, which came into affect in August 2000, authorizes the use of wiretaps for cases involving drug trafficking, gun running, mass smuggling and gang-related murders.⁶⁹ The act requires that all ISPs make a pen-register style log of all Internet communications that can be subpoenaed at any time.⁷⁰ According to the law, prosecutors, senior police officers, narcotic controllers and officials of Japan's Maritime Safety Agency can apply for warrants to use wiretaps.⁷¹ Because the Japanese are very concerned that the wiretapping law may be abused, warrants allowing for wiretaps can only be obtained from district court judges and are valid for a mere 10 days (but can be extended for up to 30 days).⁷² Furthermore, the legislation makes it obligatory for an independent third party, such as an employee of Japan's Nippon Telegraph and Telephone Company, to monitor the wiretap.⁷³ The act also makes it mandatory that individuals who have been monitored are notified within 30 days of the end of the investigation⁷⁴ and prevents law enforcement agencies from wiretapping the communications of lawyers, doctors and religious leaders.⁷⁵

Little information is known about the Royal Canadian Mounted Police's (RCMP) use of electronic surveillance since the RCMP refuses to publicly acknowledge whether they have electronic surveillance capabilities.⁷⁶ However, many believe that the RCMP is using the FBI's Carnivore surveillance system to intercept the electronic

communications of suspected criminals.⁷⁷ As the RCMP regularly works closely with the FBI on matters of mutual interest, it is certainly likely that the RCMP would take advantage of the Carnivore program to combat online criminal activity. However, the FBI claims that the Carnivore program has never been used outside the United States.⁷⁸ Yet, the FBI does admit that they would allow the RCMP to use the program if the need arose.⁷⁹

Although the FBI denies that Carnivore has been used by the RCMP, this does not mean that the RCMP is incapable of electronic surveillance. It is a known fact that the Canadian Security Establishment (CSE), a participant in ECHELON, conducts electronic surveillance. Thus the RCMP could work in conjunction with the CSE to intercept Internet communications. No matter the technology that the RCMP uses to conduct electronic surveillance, it is likely that they are capable of surveying Internet transmissions. Without a doubt information related to the RCMP's electronic surveillance capabilities will become available as surveillance of the Internet becomes widespread and intercepted electronic communications are used as evidence in Canadian courts.

On June 7 2000, the Australian government passed the Telecommunications Legislation Amendment Bill 2000 or TILAB 2000. The Bill creates two new types of warrants for electronic communication surveillance. The first, known as a "Named Person Warrant" allows law enforcement agencies to request permission to track a person's Internet activity without having to identify why or by which means they will monitor the person. The second is a special type of warrant called a "Foreign Communications Warrant" which permits law enforcement agencies to intercept electronic communications crossing Australia's border "for the purposes of collecting foreign intelligence."⁸⁰

C. Carnivore controversy

As soon as the FBI announced they developed the Carnivore electronic surveillance system critics deemed the system unlawful. Opponents of Carnivore allege that the surveillance system invades privacy, limits liberty and violates the Fourth Amendment of the US Constitution. Organizations such as StopCarnivoreNOW!, the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) have petitioned the American government to stop deployment of Carnivore.

Although the American government heard the cries of outrage regarding Carnivore, very little was done to appease the critics or address their concerns. The only initiative taken by the US Government to calm Carnivore's opponents was to commission an independent review of the Carnivore electronic surveillance system.⁸¹ Instead of shedding light on the constitutionality, the functionality and the FBI's usage of the system, the review did nothing more than enrage critics who deemed the review biased and hamstrung.

The FBI claims that use of Carnivore is permissible since electronic surveillance conducted by Carnivore is analogous to the wiretapping of telephone systems. In other words, the FBI claims that usage of Carnivore is in accordance with pre-existing laws regarding surveillance, namely Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communication Protection Act of 1986. The use of Carnivore in full-content mode is analogous to a wiretap of a telephone call, and consequently the same laws that apply to wiretaps should apply to Carnivore when it is operating in full-content mode. However, questions remain regarding whether the analogy between the operations of Carnivore in pen-mode and the operations of pen registers and trap-and-trace devices used on the telephone system is accurate.

Critics claim that use of Carnivore in pen-mode allows the FBI to access a much larger scope of data than traditional pen-registers and trap-and-trace devices used on phone systems.⁸² First, Carnivore boxes are installed on an ISP's data network and not a telephone line, therefore information collected by Carnivore is not limited to the target's communications as it is when a pen-register or trap-and-trace device is used on a suspect's private telephone line.⁸³ Furthermore, in telephone systems with digital switching technologies, out-of-band signaling is used, meaning that call routing information (transactional information) is carried on a different channel than the conversation itself (substantive information). In older analog telephone systems, transactional information and substantive data are carried on the same channel, but the signaling of transactional information, the information collected by pen-register and trap-and-trace devices, consists of pulses and tones whereas the conversation is encoded differently. Therefore, in both digital and analog telephone systems it is impossible to capture substantive information using either pen register or trap-and-trace devices.⁸⁴ However, when transmitting data over the Internet,

The FBI claims that use of Carnivore is permissible since electronic surveillance is analogous to the wiretapping of telephone systems

with the exception of FTP (File Transfer Protocol) data, both transactional information and substantive information are combined in the form of packets, making addressing information impossible to separate from content data.⁸⁵ Furthermore, since both Internet transactional and substantive data are recorded in digital form, any machine or system that can process one can process the other, such that it is impossible to be certain that the processing of transactional information does not intentionally or unintentionally divulge content data.⁸⁶

Moreover, traditional pen-register and trap-and-trace devices only collect telephone numbers. However, when Carnivore is used in pen-mode it collects the subject line and content of e-mails, replacing each character of these fields with an "X".⁸⁷ Therefore, through use of Carnivore the FBI can record the length of each data field of an electronic communication.⁸⁸ Although the length of telephone calls are legally recordable, there is nothing in the laws related to phone tapping that can be analogous to recording the length of individual data fields, as is the case with Carnivore.⁸⁹ The fact that Carnivore documents the length of individual fields might seem insignificant, yet much can be deduced from such information. For instance, take the case of a child pornography suspect, the FBI surveys his communications in pen-mode and notices that although most of his messages are small, some are extremely large, indicating that perhaps illegal pictures are being transferred. The FBI can then take the destination information of these large files and start surveying the recipients of these files as to discover a potential child pornography ring.⁹⁰ Although clearly arguable that such measures are a 'good thing', such surveillance is illegal, since developing additional leads or charges against a suspect in this fashion is impermissible without following the correct procedure for a full investigation.

In addition, e-mail addresses and URLs reveal much more information than do digits in telephone numbers.⁹¹ Telephone numbers only reveal the location from where a call is placed and the person to whom the number is registered.⁹² In contrast, e-mail addresses can reveal the identity of corresponding parties, an individual's organizational affiliations and perhaps even personal characteristics.⁹³ For instance, take one of the authors' email addresses, markperry@acm.org, markperry@mac.com and mperry@uwo.ca - revealing affiliation with the Association of Computing Machinery, which the author uses an

Apple computer and is also associated in some manner with the University of Western Ontario.

Lastly, even if use of Carnivore in pen-mode is deemed lawful, the fact that ISPs have no control over Carnivore's deployment is inconsistent with pre-existing laws.⁹⁴ The FBI retains the sole right to alter a Carnivore box's operation once it is in place. Furthermore, the FBI can do so remotely without the knowledge or the cooperation of the ISP.⁹⁵ If Carnivore's surveillance is analogous to telephone surveillance, then why is such surveillance not conducted similarly? In the world of telephone surveillance, telephone utility companies have been extremely reluctant to allow law enforcement agencies into their switching facilities in order to survey their customers.⁹⁶ Instead, telephone companies themselves have satisfied court orders and subsequently passed on subpoenaed information to law enforcement agents. Why are the same protocols not applied to ISPs in the case of Internet surveillance? After all, ISPs best understand their own network and are in the best position to lawfully comply with a court order since they have a dual duty to produce subpoenaed information and to protect their customers' interest.

It seems that for the FBI to rationalize the use of Carnivore they must implement laws specific to Internet surveillance, since the analogy between the telephone system and the Internet is too weak to uphold Carnivore's surveillance as legitimate.⁹⁷ When asked if existing laws protecting the privacy of telephone communications are enough to protect e-mail and online activities in April 2001, 62% of the survey responded that new laws need to be written to protect online privacy.⁹⁸ However, in September 2002, the same pollster reports:⁹⁹

[C]itizens are sharply divided on the question of whether the government should be able to monitor people's email and online activities. The opinion breakdown on the question is 47% of Americans believe the government should not have the right to monitor people's Internet use and 45% say the government should have that right. A majority of Internet users oppose government monitoring of people's email and Web activities.

There has been discussion regarding whether or not the Carnivore electronic surveillance system violates the Fourth Amendment of the US Constitution. Opponents of Carnivore have deemed the system comparable to "a super wiretap capable of listening to all calls placed by all customers of a telephone company".¹⁰⁰ Critics claim that Carnivore contravenes the literal interpretation, in

addition to the figurative interpretation of the Fourth Amendment. According to them, Carnivore violates the condition that a warrant must particularly describe the “place to be searched and the persons or things to be seized” given the nature of the Internet does not allow the “place to be searched” to be “particularly described”.¹⁰¹ For instance, take a targeted suspect surfing a site in California, the FBI gets a court order to intercept the Internet communications of the suspect on his ISP’s network in New York, how could the court order include the interception of his surfing activity hosted on the Californian site?¹⁰²

Critics also condemn Carnivore, stating that its usage by the FBI contravenes the Fourth Amendment’s reasonable expectation of privacy because it over collects information while being used in pen-mode. According to critics of the system, Carnivore has the potential for misuse since the software can be improperly calibrated by pushing the wrong set of radio buttons allowing the interception of more information than is subpoenaed.¹⁰³ Even, the Independent Review of the Carnivore surveillance system claims that this problem should be addressed without further delay by creating two different versions of the Carnivore system, one for pen-mode operations and the other for full-content interceptions.¹⁰⁴

However many critics believed that even if two distinct Carnivore systems were created, Carnivore would still violate the Fourth Amendment. They argue that people seek the benefits of anonymity when using the Internet,¹⁰⁵ for instance in chat rooms, where they are not susceptible to approval or contempt from third parties¹⁰⁶ and online shopping where they do not have to reveal their personal preferences, for example their waist size or their tastes in music or books.¹⁰⁷ With the use of Carnivore lurking on the Internet, Internet users will lose their anonymity and will begin to behave differently online.¹⁰⁸

In the eyes of Carnivore’s opponents, the Fourth Amendment, which was created in order to “protect the rights of Americans while they work and play on the Internet as it does in the physical world”,¹⁰⁹ is violated by Carnivore. Given the fact that “Americans use the Internet everyday to transfer vast amounts of private data, financial statement, medical records, e-mail, online reading and shopping habits, business transactions and Web surfing”¹¹⁰ they have the right to know that their personal information is being transmitted safely, without being copied by government investigators,

since the amount of sensitive information being transmitted over the Internet is enough to allow the Government to form a “granular picture of their (an internet user) interests and activities”¹¹¹ and to allow the government to develop suspicions against them. Opponents of Carnivore maintain that if the US Government does not respect its citizens’ right to privacy nothing remains to keep American society liberal and democratic.

The Independent Technical Review of the Carnivore System commissioned by the Department of Justice and undertaken by the Illinois Institute of Technology¹¹² has been subject to much criticism. Many have deemed the report biased and inadequate.

The American Civil Liberties Union (ACLU), amongst others, has “expressed substantial reservations about both the independence of the reviewers and the proposed scope of their review.”¹¹³ They claim that for the review to be truly independent it would need to be external to the Department of Justice (DoJ), which it was not since the review was overseen by the government officials who employ Carnivore (FBI & the DoJ). Furthermore, the ACLU claims that the government chosen review panel was constrained since the review team consisted of former governmental advisors, a former Clinton information policy advisor, former DoJ officials and others with backgrounds in the National Security Agency (NSA) and the Department of Treasury. The ACLU also asserts that a single one-time review of Carnivore is inadequate since Carnivore will be replaced with its progenitors and the only way to ensure full compliance of all future versions of Carnivore would be continual oversight of the system.¹¹⁴ Critics of the IITRI report also believe that the government placed unreasonable restrictions on the review panel, including limits on the information available to the reviewers and specifications for the review that are dictatorial.¹¹⁵ Consequently, critics question the conclusions of the review. According to them, even if the review was conducted in good faith, to the best of IITRI’s ability, the limitations imposed on IITRI and the financial and time constraints placed on the review cannot support a conclusion that Carnivore is correct, safe and always consistent with American Law. One report notes:¹¹⁶

Although the IITRI study appears to represent a good-faith effort at independent review, the limited nature of the analysis described in the draft report simply cannot support a conclusion that Carnivore is correct, safe, or always consistent

The Independent Technical Review of the Carnivore System has been subject to much criticism

with legal limitations. Those who are concerned that the system produces correct evidence, represents no threat to the networks on which it is installed, or complies with the scope of court orders should not take much comfort from the analysis described in the report or its conclusions.

Furthermore, the fact that the Department of Justice bestowed a “daunting list of requirement and restrictions for the review”, and retained final authority over the report drove numerous university research teams to forego the opportunity to review the Carnivore system citing that such strict control by the DoJ would prevent an independent review of the system.¹¹⁷ Among the universities that declined requests to review the Carnivore electronic surveillance system were the Massachusetts Institute of Technology (MIT), the University of California at San Diego, Dartmouth College, the University of Michigan and Purdue University.¹¹⁸

D. ECHELON

No discussion of electronic surveillance would be complete without a description of ECHELON, the term popularly used for an automated global interception and relay system, said to carry out “quasi-total surveillance” of all communications.¹¹⁹ It must be made clear that ECHELON and similar systems are outside the normal operations of law enforcement envisaged when implementing Carnivore, or surveillance under RIPA. ECHELON is ‘1984’ now, with little oversight by government or community.¹²⁰ The system is operated by intelligence agencies in the United States, the United Kingdom, Canada, New Zealand and Australia.¹²¹ The ECHELON system is primarily used and designed to intercept the Internet, fax and telephone communications of non-military targets,¹²² specifically communications relating to terrorism, organized crime, economic dealings and scientific developments.¹²³ It is rumored that the system collects as many as 3 billion communications a day,¹²⁴ and sifts through 90% of all Internet traffic.¹²⁵ Although ECHELON is the only documented global interception system, it is likely that other nations such as France and Russia also survey international communications.

It is important to note, that ECHELON, unlike Carnivore, is not designed to eavesdrop on a particular individual’s communications. Instead, the system works by indiscriminately intercepting very large quantities of communications and then distills the collected data through artificial intelligence programs to extract messages of interest from the

mass of unwanted ones.¹²⁶ The ECHELON system is composed of a chain of interception facilities located around the world that tap into all the major components of international telecommunications networks, including international telecommunications satellites (Intelsat), regional communication satellites, radio communications, and land-based communication networks (microwave and cable).¹²⁷ These globally positioned facilities are linked together such that the data they intercept is available to the other states participating in ECHELON.¹²⁸ The United States’ National Security Agency (NSA) is by far the senior partner participating in ECHELON, the agency employs over 21 000 people and has a budget of over US \$3.6 billion, a larger operating budget than either the FBI or the CIA.¹²⁹ The other partners; the Government Communications Headquarters (GCHQ) in the United Kingdom, the Communications Security Establishment of Canada (CSE) (which employs 890 people and has an operating budget of CAN \$110 million), the Defense Signals Directorate (DSD) in Australia and the Government Communications Security Bureau (GCSB) of New Zealand, share the cost of ECHELON’s operations with the NSA and make joint use of the resulting information.¹³⁰

The alliance between these five nations grew from co-operations during World War II to intercept radio transmissions and was formalized in 1948 with the signing of the UKUSA signals intelligence agreement (SIGINT), which aimed primarily to monitor the activities of the USSR.¹³¹ It wasn’t until 1971 that the UKUSA allies began ECHELON.¹³² Before then, each ally did their intelligence gathering operations independently from one another.¹³³ Under ECHELON, the task of surveying the world’s communications is divided among the participating states. The United Kingdom has the task of surveying Africa and Europe up to the Ural Mountains of the former USSR, Canada has the task of surveying the northern latitudes and the Polar Regions, Australia and New Zealand survey Oceania and the areas surrounding the Indian Ocean, and the United States surveys North and South American transmissions as well as Pacific Intelsat transmissions.¹³⁴ Known surveillance stations are located in Yakima, Washington and Sugar Grove, West Virginia in the United States, Sebana Seca in Puerto Rico, Morwenstow and Menwith Hill in England, Geraldton, Pine Gap and Shoal Bay in Australia, Misawa in Japan, Waihopai in New Zealand, Leitrim, Ontario in Canada and Bad Aibling, Germany.¹³⁵

At each of these respective stations, there is a computer known as an ECHELON “Dictionary”.¹³⁶ Each ECHELON Dictionary is programmed daily with keywords that can be anything, including names of people, locations, ships, countries, organizations, telephone numbers, subject names and Internet addresses, or any other word of interest (e.g. “nitroglycerine”) and intercepts messages containing these keywords. However, the Dictionary at each station, not only searches intercepted messages for words inputted by its parent agency, but also searches captured data for keywords entered in partner nations’ Dictionaries.¹³⁷ Whenever a Dictionary discovers a message containing a keyword of another agency, it automatically picks up the message and sends it directly to the headquarters of the agency that inputted that specific keyword.¹³⁸

ECHELON’s participatory countries intercept communications in many ways. The most common methods of interception are massive ground radio antennas, interception satellites and IP sniffer devices¹³⁹ that are capable of handling much larger quantities of data than Carnivore boxes. However, ECHELON uses many other methods to intercept telecommunication transmissions. For instance, it is believed that American divers tap into cables carrying phone calls across the sea and install surveillance devices.¹⁴⁰ Furthermore, it is believed that the ECHELON network has buildings situated along microwave and cable routes to intercept communications,¹⁴¹ and that other transmissions are captured from space using spy satellites. In addition, it has been said that ECHELON intercepts communications through “embassy collection”: ECHELON’s embassy collection program reputedly places sophisticated receivers and processors in diplomatic bags in overseas embassies, which are then used to monitor communications in foreign capitals.¹⁴²

Although, information in regards to ECHELON does exist, the US and other participating governments have gone to extreme lengths to keep details of ECHELON operations secret. The US government takes this further, and still refuses to admit that ECHELON exists, even though both Australia and New Zealand have confirmed the system’s existence.¹⁴³ As ECHELON’s existence is confirmed, many privacy organizations and individuals are now concerned about whether ECHELON follows any legal standards. In an attempt to answer this question, the Electronic Privacy Information Center sued the US government,

without success, hoping to obtain documents describing the legal standards by which ECHELON adheres, if any exist.¹⁴⁴ Unlike the Carnivore system, whose use must conform to US surveillance laws, ECHELON engages in a subterfuge to avoid legal restrictions, which many countries have in place to prevent invasions of privacy.¹⁴⁵ For instance, it is rumored that nations would not use their own agents to spy on their citizens, but instead would assign the task to the spy agency of one of the other allies participating in ECHELON.¹⁴⁶ Since the interception of communications taking place within a given country does not target the citizens of that country, a person whose messages are intercepted does not have any domestic legal protection.¹⁴⁷

It seems that the only concern raised in regards to ECHELON, in the US in particular, is whether the interception system targets domestic traffic. Even when the US Congress held hearings concerning the activities of NSA, these hearings were confined to whether US citizens were affected by NSA’s surveillance, without any real concern expressed regarding the legality of NSA’s surveillance or the existence of the ECHELON surveillance system itself.¹⁴⁸ As evidence indicates that domestic traffic is not intercepted by internal spy agencies, ECHELON continues to exist with little resistance. However, it is likely that if a US agency required information on a US citizen it could ask one of the other ECHELON facilities to oblige in gathering information. The US facility would then not be spying on a US citizen, though the effect would be the same. This technique was reportedly used by Margaret Thatcher.¹⁴⁹

E. Conclusion

Although the FBI’s Carnivore electronic surveillance system has been plagued with bad publicity and is in dire need of improvement in order to make it comply transparently with American laws regarding surveillance, it is unlikely that the FBI will stop using Carnivore. Without Carnivore or a comparable software suite, the FBI would be unable to conduct electronic surveillance. Consequently, it is evident that Carnivore is an asset to the FBI. However, the FBI seems unwilling to neither admit the shortcomings of the software nor allow that the software must be improved and its use must be subject to strict regulations such that it does not infringe upon the freedom and the right to privacy of American citizens. Currently the FBI maintains a viewpoint that public safety is by far the most important concern of Americans. Following the attack on the United States on 11

It is unlikely that the FBI will stop using Carnivore

September 2001 they face much less opposition than before that time. However, John Ashcroft, the current Attorney General of the United States, who is not known for his liberal views remarked (in relation to encryption controls):¹⁵⁰

*There is a concern that the Internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant the government the Orwellian capability to listen at will and in real time to our communications across the Web? The protections of the Fourth Amendment are clear. The right to protection from unlawful searches is an indivisible American value. Two hundred years of court decisions have stood in defense of this fundamental right. The state's interest in effective crime-fighting should never vitiate the citizens' Bill of Rights.*¹⁵¹

The first step in order to make Carnivore an acceptable law enforcement tool in the eyes of individuals concerned with their privacy, would be to address the legitimacy of the system. As it stands Carnivore disregards privacy rights. Furthermore, since current wiretapping laws do not specifically address surveillance of Internet communications, nor are they applicable by analogy to the telephone system, legislation specifically addressing the interception of Internet transmissions must be written in order to legitimize Carnivore.

Moreover, Carnivore's technical limitations must be rectified. The Carnivore program, in its current states, seems like nothing more than a benchmark project since it is plagued by technical shortcomings. The Carnivore system must be made resilient and reliant in order for it to remain an asset as a law enforcement tool in an era where technology is quickly evolving and criminals are becoming increasingly clever. The FBI must therefore invest personnel and other resources to make Carnivore bug-free, and must refrain from deploying the system until it achieves such robustness.

In addition, Carnivore is currently a burden to the technology industry, since its source code remains secret and its effects to networks undocumented. In order to appease the technology industry's concerns in regards to Carnivore, the FBI should allow and encourage ISPs to handle data interceptions themselves, using their IP sniffer program of choice, as they allow telephone utility companies to wiretap telephone calls. Furthermore, the FBI should release data regarding Carnivore to

the public, instead of waiting to divulge such information only after it is leaked to media outlets.

However, even if the FBI makes compromises in regards to Carnivore's deployment and Congress creates legislation specifically addressing the wiretapping of Internet transmissions, appeasing ISPs and individuals concerned with illegitimate governmental surveillance, it would be naïve to believe that the battle to secure individual privacy in the electronic realm had been won. Although Carnivore scandalized the FBI because of its apparent disregard for the constitutional rights of freedom and privacy of Americans, the most invasive breaches of privacy are being conducted by secret organizations and these invasions of privacy remain unknown and cannot be ended by judicial appeals. Thus, no matter what domestic policies regarding Carnivore are put in place, the existence of private communications will continue to be nothing more than an illusion, since ECHELON and other similar systems will continue to monitor them.

No matter what is done to make Carnivore lawful, it can be argued that the right to electronic privacy, a battered cornerstone of modern democracy, has already been lost forever thanks to systems like ECHELON. However, this does not mean that we should sit back, be docile, and allow democratic governments to act without restraint 'in the interests of security'. Although Carnivore is primarily a US system, undoubtedly similar software is in use or, at least, under development, in Canada. We should be ever more vigilant in the face of programs such as Carnivore and ECHELON, policies that lead to legislation such as RIPA, systems like SORM, and a growing acceptance in the face of terror in US for acceptance of a Total [Terrorism] Information Awareness program. As citizens who cherish freedom, we should unite and remind our governments that concerns for public security can rob us of our fundamental right to be free from unfettered governmental surveillance. At the very minimum we should be kept informed of the actions that the state is taking to monitor our communications or systems it is considering to implement. If we see security as part of the struggle to preserve our way of life, the security itself should not repudiate that way of life.

Talitha Nabbali BSc (Hons) Graduate 2002, University of Western Ontario and Mark Perry, Assistant Professor Faculty of Science (Computer Science) Faculty of Law University of Western Ontario; mperry@uwo.ca

FOOTNOTES

- 1 An earlier version of this article was presented at the Law Commission of Canada hosted conference In Search of Security: An International Conference on Policing & Security Montréal, Québec, Canada, February, 2003, under the title Going for the Throat: Techniques in Crime Control or Denial of Privacy
- 2 Thanks to Michael McLaren, Rob Kitto, and Pam Krauss for their research assistance, funded in part by the Law Foundation of Ontario.
- 3 J. Goodman, et al, "Carnivore: Will it Devour your Privacy?"(2001) Duke L. & Tech. Rev. 0028.
- 4 However, this may change in the US if the Total Information Awareness proposals discussed above are taken forward.
- 5 USA., Department of Justice, Carnivore and the Fourth Amendment, (Statement of Kevin V. DiGregory, Deputy Assistant Attorney General, United States Department of Justice, Before the Subcommittee on the Constitution of the House Committee on the Judiciary)(24 July 2000), online: US Department of Justice
<http://www.usdoj.gov/criminal/cybercrime/carnivore.htm> (date accessed: 24 September 2001) [hereinafter "Carnivore and the Fourth Amendment"].
- 6 S.P. Smith et al., "Independent Review of the Carnivore System – Final Report", Illinois Institute of Technology Research Institute (8 December 2000) online: US Department of Justice:
http://www.usdoj.gov/jmd/publications/carniv_final.pdf (date accessed: 26 December 2002).
- 7 Title III of the Omnibus Crime Control and Safe Streets Act of 1968 18 USC. §§ 2510-22
- 8 Carnivore and the Fourth Amendment, supra note 5.
- 9 R. Graham, "Carnivore FAQ (Frequently Asked Questions)"online: Robert Graham
<http://www.robertgraham.com/pubs/carnivore-faq.html>, (date accessed: 28 December 2001).
- 10 Smith, supra note 6.
- 11 Ibid.
- 12 Goodman, supra note 3.
- 13 Ibid.
- 14 U.S.A., Federal Bureau of Investigation, Internet and Data Interception Capabilities Developed by FBI, (Congressional Statement) by D. M. Kerr,(Washington, D.C.:24 July 2000), online: FBI
<http://www.fbi.gov/congress/congress00/kerr072400.htm> (date accessed: 24 Dec 2002).
- 15 M.M. Grier Jr., "The Software Formerly Known as 'Carnivore': When Does E-mail Surveillance Encroach Upon a Reasonable Expectation of Privacy?" (2001) 52 S.C. L. Rev. 875.
- 16 Smith v. Maryland 442 US 735, 739 (1979).
- 17 See discussion in Goodman, supra note 3.
- 18 47 USC. § 1001
- 19 D. Gessel, "CALEA, Carnivore, and Counter-measures"(IS2K Conference, Seoul, Korea, 2000), online:
http://www.dis.org/gessel/IS2K/CALEA_Carnivore.pdf (date accessed: 8 February 2002).
- 20 United States Telecom Ass'n v. FCC 227 F.3d 450, 453 (D.C. Cir. 2000).
- 21 Ibid at 455 (references omitted). See discussion in Grier, supra note 15.
- 22 21st Century Department of Justice Appropriations Authorization Act (H.R. 2215).
- 23 R. Longley, "Congress Clamps Down On Carnivore" *About.com* (6 August 2001), online:About.com
<http://usgovinfo.about.com/library/weekly/aa080601a.htm> (date accessed: 27 December 2001).
- 24 Stacy Blasberg "Legal Update: Law and Technology of Security Measures in the Wake of Terrorism" 8 B.U. J. SCI. & TECH. L. 72
- 25 D. McCullagh, "Senate OKs FBI Net Spying" *Wired News* (14 September 2001), online: *Wired News*
<http://www.wired.com/news/politics/0,1283,46852,00.html> (date accessed: 29 December 2001).
- 26 B. Sullivan, "FBI Software Cracks Encryption Wall", *MSNBC*(20 November 2001), online: *MSNBC*
<http://www.msnbc.com/news/660096.asp> (date accessed: 27 December 2001).
- 27 McCullagh, supra note 25.
- 28 Ibid.
- 29 Regulation of Investigative Powers Act (U.K.), 2000, c. 23.
- 30 Gessel, supra note 19.
- 31 K. Lillington, "Irish, UK Crypto Regs Far Apart" *Wired News* (16 February 2000), online: *Wired News*
<http://www.wired.com/news/print/0,1294,34350,00.html> (date accessed: 24 May 2002).
- 32 Regulation of Investigatory Powers Act 2000, Ch. 23, s. 2 (Eng.). See also discussion in Gessel, supra note 19.
- 33 Ibid.
- 34 The Economic Impact of the Regulation of Investigatory Powers Bill (The British Chambers of Commerce, 2000) (Editors: I. Brown, S. Davies, G. Hosein), online: The British Chambers of Commerce
<http://www.britishchambers.org.uk/newsandpolicy/ict/ripbillsummary.htm> (date accessed: 3 July 2002 – no longer online at this site, but held on file) [hereinafter "Economic Impact"].
- 35 Ibid.
- 36 Regulation of Investigatory Powers Act 2000, Ch. 23, s. 5(3) (Eng.)
- 37 Regulation of Investigatory Powers Act 2000, Ch. 23, s. 18(2) (Eng.)
- 38 R. Maddocks, "RIP No Longer Means Requiescat In Pace" *Le Québécois Libre* (1 April 2000), online: *Le Québécois Libre*
<http://www.quebecoislibre.org/000401-6.htm> (date accessed: 9 February 2002). For discussion of the Act, see "STAND's Guide to the RIP v1.0"(2 March 2002), online: <http://www.stand.org.uk/ripnotes> (date accessed: 24 December 2002).
- 39 Economic Impact, supra note 34.
- 40 Regulation of Investigatory Powers Act 2000, Ch. 23, s. 49 (Eng.).
- 41 I. Brown & B. Gladman, "The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses", online:
<http://www.fipr.org/rip/RIPcountermeasures.htm> (date accessed: 24 May 2002).
- 42 Lillington, supra note 31.
- 43 Economic Impact, supra note 34.
- 44 Ibid.
- 45 Ibid.
- 46 A. Docherty, "U.K. Crypto Law a Key Issue" *Wired News* (7 March 2000), online: *Wired News*
<http://www.wired.com/news/print/0,1294,34776,00.html> (date accessed: 24 May 2002).

- 47 J. Naughton, "Three Minute Guide to RIP" Stand (12 March 2000), online: Stand <http://www.stand.org.uk/commentary.php3> (date accessed: 24 May 2002).
- 48 Economic Impact, *supra* note 34.
- 49 *Ibid.*
- 50 *Ibid.*
- 51 *Ibid.*
- 52 Docherty, *supra* note 46.
- 53 Information Society Commission, "Key Issues : Electronic Commerce", online: <http://www.isc.ie/cgi-local/publications.cgi?f=ecomm> (date accessed: 26 May 2002).
- 54 D. Kelleher, "Legislation Strong on Privacy for Internet" *Irish Times* 11 July 2000 p 16
- 55 *Ibid.*
- 56 *Ibid.*
- 57 Economic Impact, *supra* note 34.
- 58 *Ibid.*
- 59 Graham, *supra* note 9.
- 60 Economic Impact, *supra* note 34.
- 61 *Ibid.*
- 62 *Ibid.*
- 63 See "'SORM' to Shutdown?" *Cryptome.org* Moscow, Russia (25 September 2000), online: *Cryptome.org* <http://cryptome.org/ru-sormshut.htm> (date accessed: 13 June 2002).
- 64 A. Ivanov, "Sorm Problem: Latest News" St. Petersburg Civil Law Center, online: *Balfort.com* <http://www.balfort.com/sorm.html> (date accessed: 13 June 2002).
- 65 *Ibid.*
- 66 Larisa Naumenko "Bugging Key in Hostage Battle" *The Moscow Times*, October 29, 2002
- 67 Graham, *supra* note 6.
- 68 Privacy and Human Rights 2000 : Country Reports : Japan, online: *Privacy International*, 2000 <http://www.privacyinternational.org/survey/phr2000/countrieshp.html> (date accessed: 24 June 2002) [hereinafter "Privacy and Human Rights 2000"].
- 69 *Ibid.*
- 70 "Wiretap, but Carefully" *The Japan Times Online* (28 August 2000), online: http://www.snapshot.com/www_problems/Japan/Wiretap_but_carefully.htm (date accessed: 24 June 2002) [hereinafter "Wiretap"].
- 71 Graham, *supra* note 9.
- 72 Wiretap, *supra* note 70.
- 73 *Ibid.*
- 74 D.A. Laverty, "JAPAN: Internet Privacy and Related Developments" *International Counsel* (March 2000), online: *International Counsel* <http://www.internationalcounsel.com/pubs/updates/update008.htm> (date accessed: 24 June 2002).
- 75 Privacy and Human Rights 2000, *supra* note 68.
- 76 Graham, *supra* note 9.
- 77 T. Hamilton, "FBI Software Can Take Bite Out of Canadians' Privacy" *Toronto Star* (25 March 2001), online: <http://www.etc.ca/pages/media/2001/2001-03-25-a-torontostar.html> (date accessed: 13 June 2002).
- 78 *Ibid.*
- 79 *Ibid.*
- 80 *Ibid.*
- 81 Gessel, *supra* note 19.
- 82 Smith, *supra* note 6.
- 83 Goodman, *supra* note 3.
- 84 *Ibid.*
- 85 Smith, *supra* note 6.
- 86 *Ibid.*
- 87 *Ibid.*
- 88 Goodman, *supra* note 3.
- 89 *Ibid.*
- 90 *Ibid.*
- 91 Grier, *supra* note 15.
- 92 *Ibid.*
- 93 *Ibid.*
- 94 Goodman, *supra* note 3.
- 95 Grier, *supra* note 15.
- 96 U.S.A., Centre for Democracy and Technology, *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age*, (Testimony of James X. Dempsey before the United States Senate - Senate Judiciary Committee) (6 September 2000), online: *Centre for Democracy and Technology* <http://www.cdt.org/testimony/000906dempsey.shtml> (date accessed: 25 December 2002) [hereinafter "Carnivore Controversy"].
- 97 *Ibid.*
- 98 *United States Telecom Ass'n v. FCC* 227 F.3d 450, 453 (D.C. Cir. 2000).
- 99 Susannah Fox and Oliver Lewis "Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy" *Pew Internet & American Life Project*, (2 April 2001) online: http://www.pewinternet.org/reports/pdfs/PIP_Fear_of_crime.pdf (date accessed: 27 December 2002).
- 100 Lee Rainie, Susannah Fox, & Mary Madden, "One Year Later: September 11 and the internet" <http://www.pewinternet.org/reports/toc.asp?Report=69>
- 101 Longley, *supra* note 23.
- 102 M. Rothenberg, "FBI's Carnivore Gnawing at liberty?" *ZDNN* (11 July 11 2000), online: *ZD Net* <http://www.zdnet.com/filters/printerfriendly/0,6061,26019,60-2,00.html> (date accessed: 19 September 2001).
- 103 Stop Carnivore Now, *supra* note 96.
- 104 Grier, *supra* note 15.
- 105 Smith, *supra* note 6.
- 106 Grier, *supra* note 15.
- 107 US Senate, *The Fourth Amendment and the FBI's Carnivore Program*, (Testimony before the United States Senate - Senate Judiciary Committee by Jeffrey Rosen) (6 September 2000), online: *US Senate*: http://judiciary.senate.gov/oldsite/962000_jr.htm (date accessed: 26 December 2002) [hereinafter "Fourth Amendment and FBI"].
- 108 Grier, *supra* note 15.
- 109 Fourth Amendment and FBI, *supra* note 107.
- 110 Carnivore and the Fourth Amendment, *supra* note 5.

- 111 Carnivore Controversy, *supra* note 96.
- 112 Fourth Amendment and FBI, *supra* note 107.
- 113 Smith, *supra* note 6.
- 114 C. Chiu, & B. Steinhardt, "ACL Comments regarding Carnivore review team draft report" American Civil Liberties Union (12 January 2000) online: American Civil Liberties Union <http://www.aclu.org/> (date accessed: 25 December 2002).
- 115 *Ibid.*
- 116 *Ibid.*
- 117 S.M. Bellovin et al., "Comments on the Carnivore System Technical Review", (3 December 2000), online: http://www.crypto.com/papers/carnivore_report_comment_s.html (date accessed: 27 December 2002).
- 118 R. Stenger, "Universities Unwilling to Review FBI's 'Carnivore' system – Agency's Restrictions Seen as Overbearing" CNN (6 September 2000), online: <http://europa.cnn.com/2000/TECH/computing/09/06/carnivore/> (date accessed: 25 December, 2001).
- 119 *Ibid.*
- 120 European Parliament, Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), (A5-0264/2001), online: http://www.fas.org/irp/program/process/rapport_Echelon_en.pdf (date accessed: 20 December 2002) [hereinafter "European Parliament"].
- 121 For reports on Echelon from Zdnet UK, see <http://www.zdnet.co.uk/news/specials/2000/06/Echelon/> (date accessed: 20 March 2003).
- 122 *Ibid.* See also, "Echelonwatch – Frequently Asked Questions about Echelon" American Civil Liberties Union (7 February 2002), online: American Civil Liberties Union <http://www.aclu.org/Echelonwatch/faq.html> (date accessed: 26 December 2002) [hereinafter "Echelonwatch"]. It is also clear that nations outside this group run their own systems, such as Frenchelon, see <http://www.zdnet.co.uk/news/specials/2000/06/Echelon/> (date accessed: 20 March 2003).
- 123 N. Hagar, "Exposing the Global Surveillance System" Covert Action Quarterly, online: Mirio's Cyberspace Station <http://public.srce.hr/~mprofaca/Echelon01.html> (date accessed: 16 May 2002).
- 124 J. Bronskill, "Canada a Key Snooper in Huge Spy Network" The Ottawa Citizen (24 May 1999), online: <http://insight.mcmaster.ca/org/efc/pages/media/ottawa.citizen.24may99.html> (date accessed: 29 May 2002).
- 125 Echelonwatch, *supra* note 122.
- 126 *Ibid.*
- 127 Hagar, *supra* note 123.
- 128 *Ibid.*
- 129 European Parliament, *supra* note 120.
- 130 Bronskill, *supra* note 124.
- 131 European Parliament, *supra* note 120.
- 132 Hagar, *supra* note 123.
- 133 Echelonwatch, *supra* note 122.
- 134 Hagar, *supra* note 123.
- 135 D. Campbell, "Inside Echelon" Telepolis das Magazin der Netzkultur (25 July 2000), online: <http://www.telepolis.de/english/inhalt/te/6929/1.html> (date accessed: 29 May 2002).
- 136 European Parliament, *supra* note 120.
- 137 Hagar, *supra* note 123.
- 138 *Ibid.*
- 139 *Ibid.*
- 140 Echelonwatch, *supra* note 122.
- 141 *Ibid.*
- 142 *Ibid.*
- 143 *Ibid.*
- 144 New Zealand describes the facility, with pictures, on the government website: see Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet Securing? our? Nation's? Safety? <http://www.dpmc.govt.nz/dess/securingoursafety/index.html> (date accessed: 27 December 2002).
- 145 Echelonwatch, *supra* note 122.
- 146 *Ibid.*
- 147 *Ibid.*
- 148 European Parliament, *supra* note 120.
- 149 *Ibid.*
- 150 As related by Mike Frost in CBS's 60 Minutes programme in 2000: "[Thatcher] had two ministers that she said, quote, 'they weren't onsite,' unquote ... so my boss went to London and did intercept traffic from those two ministers." See http://news.bbc.co.uk/1/hi/uk_politics/655996.stm (date accessed: 27 March 2003).
- 151 J. Ashcroft, "Keep Big Brother's Hands off the Internet" (1997) 2(4) USIA Electronic Journal, online: <http://usinfo.state.gov/journals/itgic/1097/ijge/gj-7.htm> (date accessed: 27 December 2002).