



The Law Library of Congress

REPORT FOR CONGRESS

January 2011

Global Legal Research Center
LL File No. 2011-005180

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

This report concerns whether the government may scan all Internet traffic for known malware or transmissions from known bad sites, in Australia, Canada, France, Israel, Russia, and the United Kingdom. The report supplements an earlier report on the privacy of electronic communications (LL File No. 2011-5074).

The Library of Congress
James Madison Memorial Building, 101 Independence Avenue, S.E., Room LM-240
Washington, DC 20540-3200
(202) 707-6462 (phone), (866) 550-0442 (fax), law@loc.gov (email)
<http://www.loc.gov/law>

LAW LIBRARY OF CONGRESS

AUSTRALIA

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

Executive Summary

The Telecommunications (Interception and Access) Act 1979 (Cth) does not authorize the general scanning of the Internet for malware or transmissions from known bad sites by government security or enforcement agencies. However, information and documents relating to “telecommunications data” may be obtained without a warrant and could enable the identification of the Internet Protocol (IP) addresses of the sender and recipients of such transmissions, but not access to the content of the communications. A government initiative to detect malware uses external sources of information and does not involve the relevant government agency in conducting general scans of Internet traffic.

As stated in Report No. 2011-005074 on Australia, the unauthorized access to or impairment of computer systems, including hacking, denial of service attacks (and distributed denial of service attacks), and the creation and distribution of malware, may constitute offenses under the federal Criminal Code Act 1995 (Cth)¹ and State and Territory criminal laws. In addition, the Spam Act 2003 (Cth) contains offenses relating to unsolicited commercial electronic messages.²

In investigating such offenses, the interception of online communications by law enforcement agencies is governed by the Telecommunications (Interception and Access) Act 1979 (Cth) [TIA].³ While this legislation contains provisions that allow authorized employees of Internet service providers (ISPs) to access and use electronic communications in performing duties relating to “network protection,”⁴ there is no specific authority for government agencies to generally scan the Internet for malware or transmissions from known bad sites. Furthermore, interception warrants must identify the person who is the target of the investigation and the particular telecommunications service or devices used by that person; such warrants do not authorize broad scans or monitoring of Internet traffic.

¹ *Criminal Code Act 1995* (Cth) pt 10.7, [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/3D80BF4AA572A9FFCA257801000991A6/\\$file/CriminalCode1995_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/3D80BF4AA572A9FFCA257801000991A6/$file/CriminalCode1995_WD02.pdf). Computer offenses were introduced into the Criminal Code by the *Cybercrime Act 2001* (Cth), [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/78F3C45ABCF46F42CA256F7100560110/\\$file/Cybercrime2001.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/78F3C45ABCF46F42CA256F7100560110/$file/Cybercrime2001.pdf).

² *Spam Act 2003* (Cth), [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/B300333EF232069BCA25777400815BB7/\\$file/SpamAct03WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/B300333EF232069BCA25777400815BB7/$file/SpamAct03WD02.pdf).

³ *Telecommunications (Interception and Access) Act 1979* (Cth), [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F106D44BEEE5431ACA2577EB0005DF81/\\$file/TelecommIntAccess1979_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F106D44BEEE5431ACA2577EB0005DF81/$file/TelecommIntAccess1979_WD02.pdf).

⁴ *Id.* ss 7(2)(aaa), 63C.

However, access to “telecommunications data” is subject to a less restrictive regime under Chapter 4 of the TIA. For example, the provisions allow enforcement agencies to authorize a service provider to disclose historical data if the disclosure is reasonably necessary for the enforcement of the criminal law,⁵ and may also authorize the disclosure of prospective data if the disclosure is reasonably necessary for the investigation of an offense that is punishable by at least three years’ imprisonment.⁶

“Telecommunications data” is not defined in the legislation, but it is stated that the provisions do not authorize the disclosure of information or a document that is “the contents of substance of a communication.”⁷ The explanatory memorandum to the 2007 bill that introduced Chapter 4 into the legislation states that, for Internet-based telecommunications such as “email, web browsing, instant messaging, or internet voice calls (Voice over Internet Protocol or VoIP),” telecommunications data may include “the sender’s and recipient/s’ Internet addresses, the devices from which they were sent from or to, and the time and date at which it was sent. The information does not include content such as the subject line of an email, the message sent by email or instant message or the details of Internet sessions, such as the Uniform Resource Locator/Identifier (URL/URI).”⁸ It is therefore possible to obtain general data about transmissions involving a known bad site in the context of a criminal investigation, although a warrant would be needed to obtain the content of the communications.

In terms of detecting and remediating malware (particularly “zombie” computers that are part of a botnet, or automated cyber-attack), the Australian Internet Security Initiative,⁹ which is operated by the Australian Communications and Media Authority (ACMA),¹⁰ “identifies computers operating on the Australian Internet that have been infected by malware and are able

⁵ *Id.* s 178. In addition, the Director-General of Security or other approved person within the Australian Security Intelligence Organisation may authorize disclosure under ss 175 and 176, and voluntary disclosure by providers to the Organisation or enforcement agencies can occur under ss 174 and 177.

⁶ *Id.* ss 179, 180. Under the provisions, the timeframe that the authorization for the disclosure of prospective data can be in place is limited to forty-five days. The authorizing officer must also have regard to the impact of the authorization on the privacy of the individual concerned.

⁷ *Id.* s 172.

⁸ House of Representatives, Telecommunications (Interception and Access) Amendment Bill 2007, Replacement Explanatory Memorandum 8, http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r2743_ems_e0927c96-b737-4d35-92ef-bb7afea306aa/upload_pdf/311827.pdf;fileType=application%2Fpdf. See also *id.* at 6 (stating the telecommunications data include “the Internet Protocol (IP) address used for the session and the start and finish time of each session”).

⁹ See *Australian Internet Security Initiative*, ACMA (Australian Communications and Media Authority), http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 (last visited Jan. 12, 2011).

¹⁰ ACMA is responsible for regulating broadcasting, the Internet, radio communications, and telecommunications. Its role includes investigating complaints about online content under the Broadcasting Services Act 1992 (Cth), enforcing the Spam Act 2003 (Cth), and performing a number of functions set out in the Telecommunications Act 1997 (Cth), including investigations of certain matters relating to telecommunications. See generally, *Australian Communications and Media Authority Act 2005* (Cth), [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/C5920FDF9860EE82CA2577740082744A/\\$file/AusCommandMediaAuth2005.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/C5920FDF9860EE82CA2577740082744A/$file/AusCommandMediaAuth2005.pdf). See also *Telecommunications Act 1997* (Cth), [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/24E855BE494098F4CA2578030002E268/\\$file/Tele1997_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/24E855BE494098F4CA2578030002E268/$file/Tele1997_WD02.pdf).

to be controlled for illegal activities.”¹¹ This voluntary program involves ACMA obtaining and collating information from private entities that “run honeypots, spamtraps, sinkholes and other mechanisms for the purpose of identifying compromised hosts or other malicious activities on the internet.”¹² ACMA then sends free daily reports to ISPs about the types of compromises detected at their customers’ IP addresses. The ISPs are expected to communicate with their customers regarding the presence of the infection and the steps that can be taken to remove it. The Australian Government is also considering the development of a similar program relating to compromised websites.¹³

In terms of regulating access to certain online content, such as child pornography, the Australian Government’s proposal for a mandatory ISP-level Internet filtering system remains the subject of consideration and debate. The proposed system would require ISPs to block access to a defined list of sites that have been identified as containing “Refused Classification” material.¹⁴ The Government has conducted initial tests of the system¹⁵ and has stated that a review of relevant legislation will be conducted this year in order for the necessary amendments to be finalized.¹⁶

Prepared by Kelly Buchanan
Foreign Law Specialist
January 2011

¹¹ HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS, HACKERS, FRAUDSTERS AND BOTNETS: TACKLING THE PROBLEM OF CYBER CRIME (THE REPORT OF THE INQUIRY INTO CYBER CRIME) 128 (June 2010), http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf.

¹² Australian Communications and Media Authority, Answers to Questions on Notice – Inquiry into Cyber Crime, question 2 (Oct. 21, 2009), http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub56_1.pdf. The publicly acknowledged sources are The Shadowserver Foundation, The Australian Honeynet Project, and SORBS (Spam and Open Relay Blocking System). ACMA also states that it uses its own spamtraps and honeypots.

¹³ Government Response, House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime 18 (Dec. 2010), http://www.dbcde.gov.au/__data/assets/pdf_file/0005/131468/Government_Response_to_the_House_of_Representatives_Parliamentary_Committee_Report_on_Cyber_Crime.pdf.

¹⁴ See *Internet Service Provider (ISP) Filtering*, DEPARTMENT OF BROADBAND, COMMUNICATIONS AND THE DIGITAL ECONOMY, http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering (last modified Aug. 20, 2010).

¹⁵ See *Internet Service Provider (ISP) Filtering ‘Live’ Pilot*, DEPARTMENT OF BROADBAND, COMMUNICATIONS AND THE DIGITAL ECONOMY, http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot (last modified Aug. 20, 2010).

¹⁶ Andrew Colley, *Agreement to Review Planned Internet Filter Laws*, THE AUSTRALIAN (Dec. 14, 2010), <http://www.theaustralian.com.au/australian-it/agreement-to-review-planned-internet-filter-laws/story-e6f9gaxk-1225970519522>.

LAW LIBRARY OF CONGRESS

CANADA

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

I. Privacy and the Criminal Code

Section 8 of the Canadian Charter of Rights and Freedoms states that “everyone has the right to be secure against unreasonable search or seizure.”¹ This provision has been interpreted to cover “surreptitious electronic surveillance.”² Section 184(1) of Canada’s Criminal Code, an Act of Parliament that applies throughout the country, recognizes constitutionally protected privacy rights by providing that anyone who uses an “electro-magnetic, acoustic, mechanical or other device” to willfully intercept a private communication is guilty of an indictable offense and is liable to imprisonment for a term not exceeding five years.³

There are a number of exceptions to this general rule, including ones covering cases in which the interception is authorized or “the interception is carried out by a person in possession or control of a computer system and is reasonably necessary to manage the service’s quality with respect to performance, prevent the unauthorized use of a computer, or prevent such malicious acts as destroying or altering data, rendering data meaningless, obstructing the lawful use of data, or denying any person access to data to which he or she is entitled.”⁴ Also, interception without judicial authorization is allowed in exceptional circumstances where a peace officer reasonably believes that the urgency of a situation is such that authorization could not be obtained in time to prevent an unlawful act that would cause serious harm to any person or property, and the target of the interception is one who would either commit the offense or suffer harm caused by its commission.⁵ However, there is no general exception for the detection of malware by government agents.

The Criminal Code does not authorize government officials to scan Internet traffic for malware or transmissions from known bad sites. Other potentially relevant laws, such as the

¹ Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, § 8, *being* Schedule B to the Canada Act, 1982, c. 11 (U.K.), http://laws-lois.justice.gc.ca/eng/charter/1.html#anchorbo-ga:l_I.

² R. v. Duarte, [1990] 1 S.C.R. 30, *available at* <http://scc.lexum.umontreal.ca/en/1990/1990scr1-30/1990scr1-30.html>.

³ Criminal Code, R.S.C. 1985, c. C-46, § 184(1), *as amended*, <http://laws-lois.justice.gc.ca/eng/C-46/page-5.html>. Canada does not have a separate Code of Criminal Procedure. Most procedural issues are addressed in the Criminal Code itself.

⁴ *Id.* § 184(2).

⁵ *Id.* § 184.4.

Telecommunications Act and the Privacy Act, also appear not to contain any provisions that would authorize such government actions.⁶

II. Legislative Initiatives

Two bills have been introduced in Parliament to give law enforcement greater access to Internet data. The first of these, Bill C-51, would add the Investigative Powers for the 21st Century Act to the Criminal Code.⁷ The second bill would add the Investigating and Preventing Criminal Electronic Communications Act⁸ to the Criminal Code. While both of these laws are designed to assist law enforcement in investigating computer crimes, they would not appear to give law enforcement officials any new powers to monitor Internet traffic generally.

III. Conclusion

Canadian law contains general prohibitions on the interception of private communications. In order to monitor Internet traffic, the police require authorization in all but extraordinary circumstances. Law enforcement is not specifically authorized to scan for malware.

Prepared by Stephen F. Clarke
Senior Foreign Law Specialist
January 2011

⁶ *Id.* § 184(3).

⁷ Bill C-51, 40th Parl. 3d Sess., <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4745885&Language=e&Mode=1&File=27>.

⁸ Bill C-52, 40th Parl. 3d Sess., <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4753163&Language=e&Mode=1>.

LAW LIBRARY OF CONGRESS

FRANCE

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

The following information supplements Law Library Report for Congress No. 2011-005074 on French law.

French law currently does not authorize the government to perform general scans of all Internet traffic in the country for malware or transmissions from known bad sites. Such scanning would violate the right to privacy and provisions on the secrecy of electronic communications. France's cyber defense authority, the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI), recently reemphasized that the right to privacy in electronic communications is protected by law, in a press release outlining French legislation on spyware.¹

The Ministry of Interior has set up an official portal where individuals may report any unlawful content they come across on the Internet.² "Unlawful content" is understood to mean content that is prohibited and punished by French law, not merely content that one finds offensive. Individuals may, for example, report pedophilia, incitement to racial hatred, the defense of terrorism or crimes against humanity, Internet fraud, and Internet piracy. Reports are investigated by a division of the Central Directorate of the Judiciary Police.³

As mentioned in Report No. 2011-005074, the Draft Law for the Programming and Performance of Internal Security, if passed, would allow the state to install software on computers to observe, collect, record, save, and transmit keystrokes. Such monitoring would be allowed only upon authorization by an Investigating Judge and to fight organized crime.⁴ The draft law would also require Internet service providers (ISPs) to block access to certain sites if the government considers it necessary to prevent the distribution of pornographic images of minors. After agreement by the judicial authorities, the Ministry of Interior would notify ISPs of which sites to block. The list from the Ministry of Interior would remain confidential.⁵

¹ Press Release, ANSSI, Législation en matière d'outils d'espionnage (June 7, 2010), http://www.ssi.gouv.fr/site_article232.html.

² INTERNET-SIGNALEMENT.GOUV.FR, <https://www.internet-sigalement.gouv.fr/PortailWeb/planets/Accueil!input.action> (last visited Jan. 18, 2011).

³ *Id.*

⁴ Assemblée Nationale, Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure art. 22, <http://www.assemblee-nationale.fr/13/ta/ta0417.asp> (last visited Jan. 18, 2011).

⁵ *Id.* art. 4.

Finally, ISPs may find themselves criminally liable under the Law on Trust in the Digital Economy if they do not act to prevent certain specific criminal offenses, including the defense of crimes against humanity, incitement to racial hatred, or child pornography. ISPs are required to establish a procedure that permits individuals to bring this type of content to their attention, and they must also notify public authorities. A violation of these obligations is punishable by a maximum penalty of one year of imprisonment and a €75,000 fine.⁶

Prepared by Nicole Atwill
Senior Foreign Law Specialist
January 2011

⁶ Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Law on Trust in the Digital Economy] art. 6, <http://www.legifrance.gouv.fr/> (Les autres textes législatifs et réglementaires).

LAW LIBRARY OF CONGRESS

ISRAEL

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

The following clarification supplements Law Library Report for Congress No. 2011-005074 on Israeli law.

Israeli law currently does not permit the government to generally scan all Internet traffic in the country for known malware or transmissions from known bad sites. As detailed in the earlier report, because of privacy concerns, surveillance and interception of specific records or communications require special permits.

A private member bill, the Internet and Cyber Security Agency Bill, 5770-2010,¹ was submitted to the Knesset on March 15, 2010. The bill proposed the establishment of an agency that would, with government approval, form a national policy for cybersecurity and define cyber threats, recovery plans, and priorities for research, among other things. The bill further calls for authorizing the agency to identify websites for the purpose of blocking and scanning Internet traffic in emergency situations or for reasons of state security.

The bill's explanatory notes recognize the significant threat to Israel's Internet infrastructure from possible malware and other vicious attacks that could impact the State's security forces, government and business services, and citizens.²

The bill was introduced as a private member bill and is still in preliminary stages.

Prepared by Ruth Levush
Senior Foreign Law Specialist
January 2011

¹ Internet and Cyber Security Agency Bill, 5770-2010, THE KNESSET (Israel's Parliament) website, <http://www.knesset.gov.il/privatelaw/data/18/2213.rtf> (last visited Jan. 10, 2011).

² For further information, see David Eshel, *Cyber-Attack Deploys In Israeli Forces*, AVIATION WEEK (Sept. 15, 2010), http://www.aviationweek.com/aw/generic/story.jsp?channel=defense&id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml&headline=null&next=0.

LAW LIBRARY OF CONGRESS

RUSSIAN FEDERATION

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

Russia does not have detailed Internet regulations. The general rules aimed at protecting privacy of communications and free access to information apply to electronic communications. While the protection of networks is the responsibility of owners and providers, there is no federal regulation that authorizes the government to scan all Internet traffic in cases where known malware or a computer attack has been discovered. It appears that the government may, however, perform general scanning and filtration of Internet traffic for the purpose of protecting government information systems.

No provisions in Russian law authorize the government to scan all Internet traffic in the country if known malware or transmissions from known “bad” sites have been discovered. Such a provision would jeopardize the constitutionally protected privacy of correspondence and freedom to access information. Although a number of government regulations allow for simplified access by the authorities to personal and business Internet traffic and provide stricter rules over Internet control, including Web content control in the case of emergencies, the general rules of criminal procedure apply to investigative activities and to questions of admissibility of evidence regardless of whether the evidence was obtained from the Internet. Article 15.3 of the Federal Law on Information, Information Technologies, and Protection of Information (Information Law), the main legal act in the field of information protection, states that the “usage of information or telecommunication networks for business or other activities cannot be a reason to establish additional requirements or restrictions to regulate this type of activity if it would be conducted without the usage of such networks,”¹ and bases the regulation of cyberspace in Russia on general principles of legal regulation in the public sphere.²

More definitive rules of information protection have been introduced for government information systems. The Information Law allows the federal government to establish mandatory requirements for the use of government information systems³ and provides for the adoption of special information protection requirements.⁴ Such requirements were introduced in 2010 by a Joint Decree of the Federal Security Service of the Russian Federation and the Federal

¹ Federal Law No. 149-FZ, ROSSIISKAIA GAZETA [ROS. GAZ.] [Russian Newspaper], July 29, 2009 (official publication).

² D.V. Gribanov, *K Voprosu o Pravovoi Teorii Kiberneticheskogo Prostranstva* [On Legal Theory of Cyberspace], GOSUDARSTVO I PRAVO, 2010, No. 4, at 58 (in Russian).

³ Federal Law No. 149-FZ art. 14.6.

⁴ *Id.* art. 16.2.

Service on Technical and Export Monitoring.⁵ The requirements set forth in the Joint Decree apply to information systems created or used by federal organs of the executive branch of government. While each operator or provider of a government information system is free to define methods and ways of protecting information, all information systems must

- prevent any unwanted consequences from violations of access to information;
- conduct activities aimed at preventing illegal actions regarding information;
- prevent malfunctions or any other impact on the technical abilities of an information system; and
- conduct activities to constantly monitor threats, and to record and preserve net traffic.⁶

The Decree also states that equipment used in each government information system must be able to discover malware, control access to information, recognize computer attacks, and filter and block net traffic.⁷

Prepared by Peter Roudik
Chief, Eastern Law Division
January 2011

⁵ Joint Decree No. 416/489 of Oct. 13, 2010, on Approval of Requirements for Protection of Information Contained in General Use Information Systems, ROS. GAZ., Oct. 22, 2010.

⁶ *Id.* § 11.

⁷ *Id.* § 17.

LAW LIBRARY OF CONGRESS

UNITED KINGDOM

SCANNING FOR MALWARE OR TRANSMISSIONS FROM KNOWN BAD SITES

The United Kingdom's Computer Misuse Act 1990 sets out offenses relating to unauthorized access to computer material; unauthorized access with the intent to commit or facilitate the commission of further offenses; unauthorized acts intended to impair the operation of a computer; and making, supplying, or obtaining articles likely to be used to commit computer crimes.¹ Law enforcement agencies are responsible for investigating these offenses.²

As stated in Report No. 2011-005074 on the United Kingdom, the Regulation of Investigatory Powers Act 2000 [RIPA] governs the interception and surveillance of online communications by law enforcement agencies.³ Under this legislation, domestic interception warrants must identify a person or single premise⁴ and therefore do not permit the general scanning of all Internet traffic. This legislation also provides for interception to occur without a warrant in limited circumstances, including interception by or on behalf of a person who provides a telecommunications service where it takes place for purposes connected with the operation of that service or with the enforcement of any enactment relating to its use.⁵ However, no provision authorizes the general scanning of Internet or network traffic by government agencies—for example, to detect malware or transmissions from known bad sites.

RIPA provides a less restrictive regime for obtaining communications data, including traffic data.⁶ This is data that is attached to “the communication and which serves to identify its source, destination, sender or sending and receiving equipment and other message attributes. It can be seen as the operating information supplied by the system as opposed to the content of the message being sent.”⁷ Under these provisions, it may be possible for certain public authorities generally to obtain information about communications transmitted from a site, although a warrant would be needed to access the content of those communications.

¹ Computer Misuse Act 1990, c.18, <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

² *See generally*, EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, UNITED KINGDOM COUNTRY REPORT 14-15 (Jan. 2010), <http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf>.

³ Regulation of Investigatory Powers Act 2000 [RIPA], c. 23, <http://www.legislation.gov.uk/ukpga/2000/23/contents>.

⁴ RIPA § 8(1).

⁵ RIPA § 3(3).

⁶ RIPA §§ 21-25.

⁷ VICTORIA WILLIAMS, SURVEILLANCE AND INTELLIGENCE LAW HANDBOOK 71 (Oxford Univ. Press, 2006).

According to a House of Lords report, *Personal Internet Security*, published in 2007, the detection and remediation of malware is generally considered to be the responsibility of end-users, such as through the installation of antivirus software.⁸ The Government's response to this report stated that it considers that Internet service providers also have "an important role in preventing security problems for users" and that there are things they can do to "optimize the ability of their networks to filter bad traffic."⁹

Prepared by Kelly Buchanan
Foreign Law Specialist
January 2011

⁸ SCIENCE AND TECHNOLOGY COMMITTEE, PERSONAL INTERNET SECURITY, 2006-07, H.L. 165-I, at 24, <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>.

⁹ HOME SECRETARY, PERSONAL INTERNET SECURITY (REPLY TO THE FIFTH REPORT FROM THE HOUSE OF LORDS SCIENCE AND TECHNOLOGY COMMITTEE), 2007, Cm. 7234, at 4, <http://www.official-documents.gov.uk/document/cm72/7234/7234.pdf>.