

Sentinel Watch List

Current as of 19 September 2005

Top Issues of Concern

- Identity Theft
- Cybercrime: Industrial Espionage, “Bot” Networks, “Phishing” and “Pharming”
- Counterfeit Goods
- U.S-Canada Small Arms Smuggling

Prepared by Richard Bruneau, Stewart Prest and David Carment of CIFP for CISC
www.carleton.ca/cifp

Topic Description and Analysis

Topic: Identity/Data Theft

Last Updated: 19 September 2005

Threat Level and Rate of Change: High and increasing

Key Developments: Recent surveys indicate that at least one in ten and possibly as many as one in five Americans have been a victim of some form of identity theft. Canadian statistics may be similar. In addition, media reports of identity theft have proliferated in recent months; however, this trend is partially offset by an increasing number of arrests and successful prosecutions related to identity theft.

Analysis: Identity theft is quickly becoming the primary criminal threat to anyone living in an information-based economy. It is useful to place identity thieves in one of two groups. The first group employs non-web based methods to obtain identity information. Such methods often require some level of physical contact with the victim's property; examples include dumpster diving, mail fraud, debit and credit card scanning, or insider access to client accounts. The second group employs web-based methods to obtain identity information; common techniques include "phishing", "pharming", keylogger software, and other forms of spyware. Recent media reports have highlighted a number of successful police initiatives against members of the former group; police forces in Canada have repeatedly demonstrated the ability to successfully investigate such cases. However, identity thieves that use web-based methods to gather proprietary information present a very different challenge to the enforcement community. Investigations targeting such criminals require resources far beyond those available to most enforcement agencies and routinely cross regional or even national borders. Cases of successful prosecution have typically depended on high-level cooperation between national police forces, private security agencies, and large software vendors such as Microsoft.

As a developed nation with a strong information-based economy, Canada must ensure that it devotes sufficient resources to investigations of both types of identity theft. The latter group, though more difficult to apprehend and prosecute, arguably pose the greater threat to Canadian citizens, businesses, and governments. Effective policing will require a highly diversified approach, ranging from consumer education and vigilance, through increased market regulation, to enhanced and targeted enforcement strategies involving cooperation with foreign enforcement agencies and the private sector whenever necessary and appropriate.

Potential Impact: Estimated costs of ID theft to Canadian consumers and businesses range as high as CD\$2.5 billion a year and growing. The potential costs are staggering if current trends continue unchecked.

Potential Timeline: Identity theft is already taking place in Canada and will continue to affect a growing number of Canadians through the medium to long term.

International Aspects: Identity theft, even that involving low-tech methods, is virtually a borderless crime. Canadians present a tempting target to identity thieves operating abroad. At the same time, there are cyber-perpetrators located here in Canada targeting victims both locally and internationally. Canadian enforcement agencies must cooperate with their international counterparts in order to effectively police against such activities.

Strategic Gaps / Key Questions: A strategic analysis of identity theft must attempt to identify the true extent of the problem in Canada, and the extent to which it is caused by actors under Canadian jurisdiction. Any enforcement effort must be a dynamic effort, as identity theft techniques quickly and constantly evolve. Finally, it must also assess the extent to which the problem can be addressed through increased policing, as opposed to enhanced private data security, consumer education, and regulatory and legislative changes.

[Click here for sources on identity theft...](#)

Topic: Cybercrime – Phishing, Pharming, Worms, etc.

Last Updated: 19 September 2005

Threat Level and Rate of Change: High and increasing

Key Developments: Cyber-crime techniques continue to evolve extremely quickly. Already the number of large-scale phishing attacks appears to be declining, even as more sophisticated and customized “spear-phishing” attacks are becoming prevalent. Other methods of attack are emerging that defy detection even by wary and well-educated computer users.

Analysis: Police forces and private internet security firms are finding themselves hard-pressed to keep up with the rapidly shifting attacks; techniques employed by cyber-criminals continue to diversify. For instance, the current trend of “spear-phishing” targets specific individuals within a given corporation, sending them a well-crafted fraudulent e-mail; this missive often effectively mimics an internal company document. The e-mail generally requests sensitive proprietary information. Such attacks are quickly replacing the random phishing expeditions that were considered the dominant form of e-mail fraud as recently as late July.

There is some disagreement over the extent to which hackers have organized into so-called “cybergangs”. Some recent reports suggest that, despite widespread evidence of cooperation among hackers, the community remains highly decentralized. Cooperation may instead be occurring on a modular basis. In the modular model, an individual or small group bankrolls a given hacking operation, hiring individuals to carry out assorted tasks on a freelance basis. The various participants communicate very little with one another, and may never physically meet. If this model is accurate, these loose associations will prove highly resistant to police action, permitting a high degree of flexibility and adaptability while presenting few obvious focal points for effective police investigation.

The threat posed by hackers is thus manifold, presenting a significant challenge to enforcement agencies everywhere. It is unlikely that police forces will be able to contain the threat independently of foreign counterparts and the private sector.

Potential Impact: Internet-based crime significantly impacts all Canadians through both compromised privacy, and disruption of commerce and trade.

Potential Timeline: Impact already being felt, and effects will likely increase over the short to medium term.

International Aspects: Canada’s open and affluent society is already not only a primary target of online crime but is also host to a number of Canadian hackers operating both locally and globally. Beyond Canada’s borders, Brazil, Bulgaria, China, Estonia, Hungary, Indonesia, Japan, Latvia, Malaysia, North Korea, Romania, Russia, and the United States have all been recently identified as “hot-spots” of online criminal activity. With the possible exceptions of the U.S. and Japan, it is likely that many schemes

originating in these countries target foreign jurisdictions – such as Canada – where the potential for profits is much higher.

Strategic Gaps / Key Questions: Despite the number of incidents documented in North America, the full extent of the problem is still in many ways poorly understood. A balanced analysis of the threat, including the current extent of the problem and likely patterns of future evolution, would provide some much-needed objectivity to the discussion. An analysis should consider the whether the current resources and legislation in place to police internet crime are sufficient to the task.

[Click here for sources on cybercrime...](#)

Topic: Counterfeit Goods

Last Updated: 19 September 2005

Threat Level and Rate of Change: Moderate and increasing

Key Developments: Recent survey evidence suggests that trade in counterfeit goods is becoming normalized in the U.K. and other Western nations.

Analysis: A recent survey in the U.K. indicated that 73% of Britons reported seeing counterfeit goods for sale, with 34% admitting to purchasing counterfeit items at one time or another. Such responses indicate a growing acceptance of counterfeit goods, one that threatens the smooth operation of an economy dependent upon respect for intellectual property. Police in Canada must work diligently to guard against a similar normalization here in Canada.

Potential Impact: The total counterfeit industry in Canada estimated by some at \$20 billion per year. This number is likely to increase.

Potential Timeline: Effects are currently being felt, and likely to increase over the short-to medium term.

International Aspects: The problem affects both Canadian firms marketing goods abroad and Canadian consumers hit by counterfeit goods entering the domestic market.

Strategic Gaps / Key Questions: To what extent does the proliferation of counterfeit goods in Canada mirror the experience in other jurisdictions such as the U.S. and U.K.? If tolerance of counterfeit goods remains lower in Canada than in the U.K, how can the enforcement community best guard against encroaching acceptance? If acceptance levels are comparable, what can be done to reverse the trend? Can local enforcement tactics be made more effective in isolation, or does effective policing depend primarily on enhanced international cooperation among enforcement agencies in both target and supply countries?

[Click here for sources on counterfeit goods...](#)

Topic: US-Canada Small Arms Smuggling

Topic: Small Arms Smuggling

Last Updated: 19 September 2005

Threat Level and Rate of Change: Moderate and stable

Key Developments: A recent series of high-profile shooting incidents in Toronto has increased public awareness of trans-border gun smuggling. However, statistics indicate that the number of gun seizures both at the border and on Toronto streets has remained relatively stable in recent years. Estimates regarding the percentage of illegal guns in Canada that originated in the U.S. vary from 50% to 80%.

Analysis: Though gun-related violence is generally decreasing in Canada, it continues to be a problem in areas populated by street gangs and other organized criminal groups. Incidents of violent crime pose grave hazards to those directly involved, to bystanders caught in the crossfire, and to enforcement officers required to respond. Unfortunately, accurate information regarding the number of illicit weapons in Canada and the rate at which they are being smuggled into the country is extremely difficult to obtain. As a result, there is considerable disagreement regarding the extent to which the recent outbreak of gun violence in the Toronto area is a symptom of increased gun smuggling across the U.S. border. Some suggest that the heightened level of violence is primarily a consequence of the evolving culture in several Toronto gangs. Members of these gangs currently seem to place an extreme emphasis on respect, willing to sacrifice of their own and others' safety in order to prove themselves or save face.

Such considerations notwithstanding, gun smuggling clearly remains a serious issue in Canada. Personal vehicles and transport trucks, First Nations territories straddling the Canada-U.S. border, and the mail system are all used to bring handguns into the country. Firearms from the U.S. are sometimes obtained in exchange for drugs from Canada – marijuana flows south, while cocaine and firearms move north. The relative lack of large-scale seizures indicates that such weapons enter the country in small shipments, perhaps just one or two at a time. Given the widespread availability of guns in the U.S., and the lack of any obvious chokepoints in the diverse supply chain, small arms smuggling will continue to present a daunting challenge to the enforcement community for the foreseeable future.

Potential Impact: Illicit small arms heighten the risk armed robbery and violent crime; they also may intensify conflicts among criminal organizations in Canada, particularly among street gangs with a demonstrated propensity for extreme violence.

Potential Timeline: Smuggled small arms will continue to pose a threat to Canadians for the medium to long term.

International Aspects: Many illicit small arms enter the country from the U.S., where such weapons are legal.

Strategic Gaps / Key Questions: To what extent are illegal small arms in Canada the result of trans-border smuggling? Are current enforcement methods sufficiently effective at preventing gun proliferation, or are there alternative tactics capable of reducing the number of new weapons entering the country each year? Are newly announced policing countermeasures in Toronto successfully containing that city's problem?

[Click here for sources on small arms smuggling...](#)

Appendix A: Principal Topic Scan Sources

News Sites

Google News Alerts www.google.com/alerts One of the best ways to automatically track news by any combination of words or phrases in almost all online newspapers and news sites around the world.

CBC www.cbc.ca/news With national and local coverage for the major centres, CBC is one of the principal sources of original news in Canada.

Canadian Press <http://www.cp.org/english/online/full/National/national.html>
Newswire service with original news from Canada

Associated Press <http://hosted.ap.org/dynamic/fronts/HOME>
Original source of newswires from around the world

Reuters www.reuters.com Another other primary source of original newswires from around the world.

BBC <http://news.bbc.co.uk> One of the best gateways of international news.

Wired www.wired.com A useful site for crime involving new technologies. Excellent hacking news and computer scam stories available here, including original reporting.

Prime Time Crime <http://www.primetimecrime.com/> A useful compilation of crime news headlines updated almost daily from across Canada and some from the US. Links are provided to stories on news sites. Maintained by a former Canadian police officer.

New York Times www.nytimes.com National US coverage and local New York news.

Los Angeles Times www.latimes.com A key look into crime issues on the US West Coast, the local news being especially useful.

Police Services

RCMP national & provincial branches www.rcmp.ca Their news release sections are key sources of information on busts and criminal activities.

City police services across Canada [http://www.mjpolice.ca/Police links.htm](http://www.mjpolice.ca/Police%20links.htm) (list of links to most city police forces across Canada) Sometimes not updated frequently, but can be a source of some bust data and other information.

INTERPOL <http://www.interpol.int> Especially useful for background on different issues. Not a lot of recent news.

Internet Security and News Sites

Anti-Phishing Working Group, <http://www.antiphishing.org/newswire.html> Membership includes financial institutions, ISPs, retailers, law enforcement agencies; works to eliminate online frauds and scams and provides a newswire regarding online criminal activity.

Computer Crime Research Center www.crime-research.org Located in Ukraine, dedicated to research of legal and criminological problems associated with emerging cybercrime.

I.D. Theft Center <http://www.idtheftcenter.org/index.shtml> A not-for-profit providing support services to victims of I.D. theft; also has some resources for law enforcement.

IDefense.com http://www.idefense.com/ An internet security company specializing in cyber-threat assessment.
Kaspersky Lab http://www.kaspersky.com Specializes in online threats including viruses, hacking, and spam. Releases a monthly survey of the top viruses worldwide
F-Secure http://www.f-secure.com/ Focuses on data protection, anti-intrusion, and spam protection. Provides an analysis and summary of worldwide data security twice annually.
McAfee http://www.mcafeesecurity.com/ Internet security company; recently released a study of criminal activity online.
PC Magazine www.pcmag.com Tech News site.
PC World www.pcworld.com Tech news site.
Postini www.postini.com E-mail and messaging security company. Provides updates on recent phishing and pharming attacks
Prolexic Technologies http://www.prolexic.com/ Focuses on macro internet analysis, providing informations on zombies and botnets.
SANS Institute www.sans.org Computer security. Publishes a monthly top-20 list of internet threats.
Sophos.com www.sophos.com A computer security services company; provides news and updates on computer and internet based threats, as well as a list of current worms and trojans on the internet.
VNUnet www.vnunet.com Tech news site.

Human Trafficking Resources

Department of Justice Canada , http://canada.justice.gc.ca/en/fs/ht/
Office of the U.N. High Commissioner for Human Rights http://www.ohchr.org/english/issues/trafficking/index.htm Special Rapporteur on trafficking in persons, especially in women and children
U.S. Department of Health and Human Services "Campaign to Rescue and Restore Victims of Human Trafficking", http://www.acf.hhs.gov/trafficking/index.html
U.S. Department of Homeland Security, Bureau for Immigration and Customs Enforcement http://www.ice.gov/graphics/index.htm
U.S. Department of Justice , http://www.usdoj.gov/trafficking.htm
U.S. Department of State , http://usinfo.state.gov/gi/global_issues/human_trafficking.html
The Asia Foundation , "Anti Trafficking in Persons in Asia Web Portal," www.tipinAsia.info

Useful Background and Analysis Sites

Australian Institute of Criminology http://www.aic.gov.au/ A very good source of statistics, trend analysis, backgrounders and more.
Institute for International Research on Criminal Policy http://www.ircp.be/uk/index.asp Especially useful for in-depth publications on European criminal trends and research methodologies.
Safecanada.ca http://www.safecanada.ca/topic_e.asp?category=2 A good source of background information and links to key sites.

Appendix B: Specific Source List for Topics

ID Theft

- Australian Broadcasting Corporation, "Identity theft warrants access re-think, says Ruddock," 15 August 2005, <http://www.abc.net.au/news/newsitems/200508/s1438064.htm> accessed 17 September 2005.
- Canadian Press, "Debit card Skimming Costs Canadian Banks \$60M," *The Kitchener-Waterloo Record*, 29 July 2005, p. A3
- Computer Crime Research Center, "Computer crime: credit card criminal ring exposed," 22 July 2005, <http://www.crime-research.org/news/22.07.2005/1379/> accessed 10 September 2005.
- Global Edmonton, "Identity theft a growing concern," 14 September 2005, <http://www.canada.com/search/story.html?id=ed91f473-23ae-40c2-aca2-d31f0481d8f5> accessed 15 September 2005
- Jaques, Robert, "One in five hit by identity theft," *VNUnet.com* 4 Aug 2005, <http://www.vnunet.com/vnunet/news/2140768/identity-theft-gallup-experian> accessed 19 September 2005.
- Mark, Roy, "ID Theft Bill Wends Through Senate," 28 July 2005, <http://www.internetnews.com/bus-news/article.php/3523801> accessed 15 September 2005.
- Marson, Ingrid, "ID theft ring hits 50 banks, security firm says," *CNET News.com*, 8 August 2005, <http://news.com.com/ID+theft+ring+hits+50+banks,+firm+says/2100-7349-3-5823591.html> accessed 10 September 2005.
- Marson, Ingrid, "'Massive' identity theft ring uncovered," *ZDNet UK*, 8 August 2005, <http://news.zdnet.co.uk/internet/security/0,39020375,39212451,00.htm> accessed 18 September 2005.
- Mbaho, William, "Identity-theft ring shut down, Mounties say," *Globe and Mail*, 31 August 2005, S2
- Merrill, Mercer, "Insurance helps with identity theft," *News 14 Carolina*, 2 August 2005, http://www.news14charlotte.com/content/local_news/?AC=&ArID=99217&SecID=2 accessed 15 September 2005.
- Millman, René, "More spyware used in identity theft," *SC Magazine*, 15 September 2005, <http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=62f3a7eb-1e23-4a6a-8a52-dac269c033cc&newsType=News> accessed 20 September 2005,
- Office of the Massachusetts Attorney General, "Pennsylvania Woman Pleads Guilty to Identity Theft Charges," 18 July 2005 <http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1446> accessed 15 September 2005.
- Office of the New Jersey Attorney General, "Division of Criminal Justice Charges State Trooper With Identity Theft & Credit Card Fraud," 19 July 2005, http://www.state.nj.us/lps/dcj/releases/2005/stolinski_0719.htm accessed 15 September 2005.
- People's Daily Online, "Indian Navy restricts movements of 3 officials over data theft" 4 August 2005, http://english.people.com.cn/200508/04/eng20050804_200122.html accessed 15 September 2005.

Red NOVA, "The Scots Hacker 'Who Crippled the U.S. Battle Fleet From His Bedroom'; Computer Infiltrator Struck in Wake of Sept 11, Court is Told," 30 July 2005, reprinted from the London Daily Mail

http://www.rednova.com/news/technology/192253/the_scots_hacker_who_crippled_the_us_battle_fleet_from/ accessed 10 September 2005.

Telegraph.co.uk, "ID cards 'will not curb identity theft' as fraudsters move with the times," 4 September 2005,

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/09/05/nid05.xml&sSheet=/news/2005/09/05/ixhome.html> accessed 19 September 2005

UPI, "Medicare, Defense cards boon to ID theft," Science Daily, 17 September 2005, <http://www.sciencedaily.com/upi/?feed=TopNews&article=UPI-1-20050917-20070200-bc-us-identitytheft.xml> accessed 20 September 2005.

Washington Post, "Marketer Found Guilty Of Data Theft," 13 August 2005,

<http://www.washingtonpost.com/wp-dyn/content/article/2005/08/12/AR2005081201745.html> accessed 15 September 2005.

Hacking and Cybercrime

Baard, Mark, "IE 7.0 may usher in wave of RSS exploits," 6 September 2005, SearchSecurity.com,

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1121852,00.html accessed 19 September 2005.

Bauknight, Trevor, "Spear-Phishing - New Angles On An Old Game," webpronews.com, 19 July 2005, <http://www.webpronews.com/it/security/wpn-23-20050719SpearPhishingNewAnglesOnAnOldGame.html> accessed 10 September 2005

Bergstein, Brian, "ATM cards at extra risk for fraud," The Cincinnati Post, 3 August 2005, <http://news.cincypost.com/apps/pbcs.dll/article?AID=/20050803/BIZ/508030337/1001>, accessed 10 September 2005.

Bridis, Ted, "Phishing underworld flourishing online," Inside Bay Area, 18 September 2005, http://www.insidebayarea.com/businessnews/ci_3040767 accessed 20 September 2005.

Canadian Press, "Government office robbed of document materials," Globe and Mail, 16 September 2005, p.S3

Cassavoy, Liane, "Web of crime: Internet gangs go global," Globe and Mail, 26 August 2005,

<http://www.globetechnology.com/servlet/story/RTGAM.20050825.gtsecurityaug25/BNStory/Technology/> accessed 19 September 2005.

CBS, "Worm Burrows into Network Flaw," 17 August 2005,

http://wcbstv.com/business/finance_story_229084208.html accessed 1 September 2005

Gameshout News, "Yahoo! Messenger under seige from Phishing attack," 12 August 2005, <http://www.gameshout.com/news/032005/article663.htm> accessed 15 September 2005.

Keizer, Gregg, "Researcher Describes How The Phishing Economy Works," Information Week, 29 July 2005,

<http://www.informationweek.com/story/showArticle.jhtml?articleID=166403892> accessed 10 September 2005.

Keizer, Gregg, "Silent, Deadly Forms Of Phishing On The Rise," Information Week, 3 August 2005, <http://informationweek.com/story/showArticle.jhtml?articleID=167100720> accessed 10 September 2005.

Koprowski, Gene J., "Feds Eye New Mission: Zombie Hunting," TechNewsWorld 30 July 2005, <http://www.technewsworld.com/story/44977.html> accessed 1 September 2005

Kotadia, Munir, "Hosting sites help hackers recruit 'zombies'," ZDNet Australia 27 July 2005, http://www.zdnet.com.au/news/security/soa/Hosting_sites_help_hackers_recruit_zombies_0,2000061744,39204129,00.htm accessed 1 September 2005

McMillan, Robert, "Is Google Exposing You to Hack Attacks?" PC World, 2 August 2005, <http://pcworld.about.com/news/Aug022005id122066.htm> accessed 1 September 2005.

O'Brien, Timothy "New Kind of Criminal is Prowling the Web," International Herald Tribune, 8 August 2005, <http://www.ihf.com/articles/2005/08/07/business/thugs.php> accessed 19 September, 2005.

Paul, Peralte C., "Phishing' scams target new waters," TheState.com, 20 July 2005, <http://www.thestate.com/mld/thestate/business/12175190.htm> accessed 10 September 2005.

PRNewswire, "Panda Software Reports on comprehensive Cybercrime Phishing Attack and Information Theft in a Single Trojan," 30 August 2005, <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/08-30-2005/0004096699&EDATE=> accessed 15 September 2005.

Quainton, David, "Katrina heralds wave of phishing fraud," SC Magazine, 6 September 2005, <http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=f836bac6-5708-4272-99dd-77db49a5714b&newsType=News> accessed 10 September 2005.

Reuters, "Brazil police arrest 85 in crackdown on hackers," 26 August, 2005, <http://msnbc.msn.com/id/9085008/> accessed 19 September 2005.

Sanders, Tom, "Phishing emails go formal: New method hides the true web address," vnunet.com, 2 August 2005, <http://www.vnunet.com/vnunet/news/2140637/phishing-emails-formal> accessed 10 September 2005.

SANS Institute, "SANS Top20 Q2 2005 Critical Vulnerability Update," 25 July 2005, <http://www.sans.org/top20/q2-2005update/> accessed 1 September 2005

SAP Info, "Zotob Hackers Arrested In Morocco and Turkey," 29 August 2005, <http://www.sapinfo.net/index.php4?ACTION=noiframe&url=http://www.sapinfo.net/public/en/news.php4/Category-28813c6138d029be8/page/0/article/Article-164514312d0ae7b07b/en/articleStatistic> accessed 19 September 2005.

Silicon Valley North, "Customized attacks jump 50 per cent as new phishing threats emerge," 2 August 2005, <http://www.siliconvalleynorth.com/home/newsAFwhVaXmFe20050802.html> accessed 10 September 2005.

Thomson, Iain, "Hackers fight to create world's largest Botnet," VNUnet.com, 18 August 2005, <http://www.vnunet.com/vnunet/news/2141275/worm-war-horizon> accessed 19 September 2005.

Walker, Leslie, "Sophisticated hackers," Deccan Herald, 8 August 2005, <http://www.deccanherald.com/deccanherald/aug82005/eb11442200587.asp> accessed 19 September 2005.

Webhosting.info, "Postini Reports Decrease in Phishing Attacks," 2 September 2005, http://www.webhosting.info/news/1/postini-reports-decrease-in-phishing-attacks_0902056404.htm accessed 15 September 2005.

Counterfeit Goods

4NI, "Counterfeit goods 'undermining' retail sector, says Minister," 30 June 2005, <http://www.4ni.co.uk/industrynews.asp?id=42051> accessed 15 August 2005

BBC News, "Boot sale counterfeiters targeted," 21 August 2005, http://news.bbc.co.uk/2/hi/uk_news/4171266.stm accessed 10 September 2005

Brown, Colin, "Bra Wars breakthrough marred by fake goods row," 6 September 2005, <http://news.independent.co.uk/business/news/article310616.ece> accessed 10 September 2005.

Chodun, Cheryl, "Police Bust Warehouse Full of Counterfeit Goods," WXYZ Action News, 27 July 2005, http://www.wxyz.com/wxyz/nw_local_news/article/0,2132,WXYZ_15924_3958361,00.html accessed 10 September 2005

Government of Hong Kong, "\$1.5m in counterfeit goods seized, 21 arrested," 2 September 2005, <http://www.news.gov.hk/en/category/lawandorder/050902/html/050902en08007.htm> accessed 10 September 2005

New Zealand National Business Review (NBR), "Home Shop fined \$12,000 for sale of counterfeit goods" 30 June 2005, http://www.nbr.co.nz/home/column_article.asp?id=12308&cid=4&cname=Business%20Today accessed 1 September 2005

Punch, Linda, "Bogus Brands and the Internet," Internet Retailer, August 2005, <http://internetretailer.com/article.asp?id=15631> accessed 1 September 2005

TheAsianNews.co.uk, "E-bay fakes den raided," 29 July 2005, http://www.theasiannews.co.uk/news/s/191/191785_ebay_fakes_den_raided.html accessed 1 September 2005

The Channel Times, "EIPR Busts Fake D-Link Product Racket," 2 September 2005, http://www.channeltimes.com/channeltimes/jsp/article.jsp?article_id=5760&cat_id=752 accessed 10 September 2005.

Thomson, Adam, "Paraguay fights war on counterfeit goods," Financial Times, 8 September 2005, <http://news.ft.com/cms/s/db88ea42-209f-11da-81ef-00000e2511c8.html> accessed 10 September 2005.

U.K. Organised Crime Task Force (OCTF), "Fake Nation ? - A study of everyday crime," 29 June 2005, <http://www.octf.gov.uk/publications/PDF/1150%20IPTOC%20Report.pdf> accessed 15 August 2005.

Small Arms

CNN.com "Weapons arrest at U.S.-Canadian border," 14 August 2005, <http://edition.cnn.com/2005/US/08/13/canada.weapons/> accessed 1 September 2005.

Freeze, Colin "Statistics belie flood of guns from U.S." The Globe and Mail, 15 August 2005.

Gillis, Charlie, "American guns, Canadian violence," Maclean's 10 August 2005, http://www.macleans.ca/topstories/canada/article.jsp?content=20050815_110483_110483, accessed 20 August 2005.

Macleans.ca "Ontario to do blitz inspections of gun shops, ask for guns to be turned in," 1 September 2005, <http://www.macleans.ca/topstories/politics/news/shownews.jsp?content=n090135A> accessed 5 September 2005

Matas, Robert, "U.S. border posse sets sights on 49th parallel," The Globe and Mail, 12 August 2005, p. A1

SENTINEL WATCH LIST

Walton, Dawn, "U.S. citizen accused of trying to smuggle guns," 29 July 2005, Page A10