SUBMISSION NO. 10

3965 Freedom Circle
Santa Clara, CA 95054

800.338.8754 main

www.mcafee.com

McAfee Response to the Parliament of Australia House of Representatives
Re: Inquiry into Cyber Crime

McAfee applauds the Government of Australia for reviewing these very important questions and concerns. We applaud the work reflected in the Australasian Identity Crime Policing Strategy which acknowledges identity theft as a pervasive, and costly reality which our citizens face here – and globally. These guidelines and work plan to come to aid of victims of identity theft are important and are a very real part in addressing one of our society's significant challenges.

a) nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans;

Overall Trends: Society's use of the internet and mobile devices is changing rapidly and *enhance* the effectiveness of increasingly sophisticated malware. Reliance on web searches and browsing, on high-capacity storage devices (iPods, USB dongles, iPhones, Blackberries) with personally identifiable information (PII), and upon social networking sites all play a role. This applies not only to the consumer base, but also to the governments and the businesses who are responsible for the security of citizen information. The fact that Australian society relies more on mobile devices than many other regions, including the U.S., suggests that more attention will need to be placed upon mobile device as vector for evolving threats. Already, as noted, the mere storage capacity of mobile devices makes them a walking opportunity for data theft. Their small form factor means easy loss or theft. Today, many IT departments still do not incorporate mobile devices in their employee training and data protection policies. The growth in malicious programs (malware) and social engineering tactics are designed to take advantage of these societal realities.

Malware: Indeed, malicious programs (malware) designed to steal personal data was up to 1.3 million unique programs in 2008 *(up from 130,000 in 2007*), a ten-fold increase, typically targeting credit card numbers and national identification numbers (*Malware Grows 10-fold in 2008*).

Economic impact: The growing number of victims and damages worldwide is staggering:

- In the U.S., identity theft victimized 8.1 mi Americans in 2008 and cybercrime cost consumers more than $7 billion during the last two years (Consumer Reports)
- In the U.K., cybercrime is estimated to cost the country "hundreds of millions every year," while retailers lost "more than £270m in 2007

from internet fraud". "(http://news.bbc.co.uk/2/hi/technology/7697704.stm)

- In Australia, as you know, cybercrime cost businesses $600 million (http://www.computerworld.com.au/article/306743/cybercrime_costs_business_600m_report?fp=16&fpid=1).
- While the emotional damages, and the time - from noting the crime to putting credit freezes on accounts, re-establishing accounts where identities are lost, and getting credit scores back to original standing - cannot be accurately estimated, costs just for the cleanup of the machine itself add up. Just simple virus removal services can cost a consumer from $90 US (McAfee virus removal service) to $300 US (Geek Squad in-home threat removal service).

Impact from Social networking: The growth in social networking and the implicit trust in these communities has given rise to new threat vectors in places like Facebook, Twitter and YouTube. Facebook and other social networking sites do not vet the community's shared programs for security issues, while Twitter and others have been plagued by a number of issues. Within these communities, threats now travel faster due to the enormous amount of trust their users place in one another. Because these web 2.0 generation of applications and websites provide enormous value to their user base, it is important to embrace them while also determining the best way to ensure these communities improve their safety for online users, and that the users themselves understand the implications. As when societies begin relying upon email in earnest, and virus education began in earnest, a similar urgent level of education is necessary for the use of web 2.0.

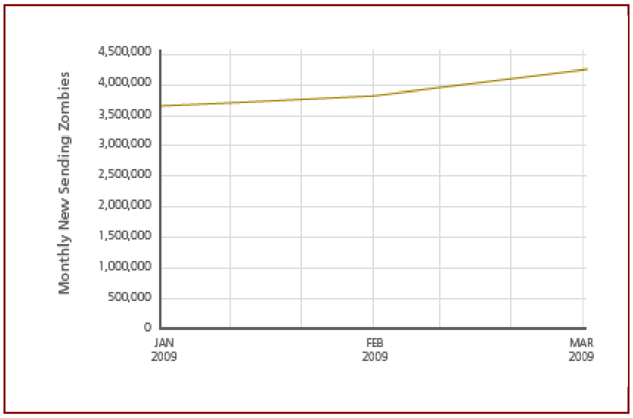
Web as vector: The growth of consumer, business and government reliance on the web for basic browsing and search has given rise to a greater level of exposure to vulnerabilities from malicious websites. "The widespread use of highly interactive 'rich client' web applications for e-commerce, business networking, and online collaboration has finally catapulted web browsers from straightforward HTML viewers to a full-blown software platform. And as corporate users are performing a significant portion of their work on the web, whether it's researching or collaborating, the safety of the underlying platform is critical to the company's success." (*McAfee, "Web Browsers: An Emerging Platform Under Attack").* While many users know the spyware dangers of downloading free screensavers and games, standard web searches are not viewed with as much scrutiny. The web is creating a new playground for cybercrime. By using social engineering tactics, criminals now entice users to malicious websites based on their desire for basic information such as health-related assistance to information about local and global news such as presidential elections, globally-impacting and events such as the Beijing Olympics. Cybercriminals are well-versed in using search statistics to build new websites hosting this malicious software, skewing search stats, and leaving users unaware of the dangers they have inadvertently encountered online. Popular search terms are used to advertise and drive (search query) traffic to a malicious website. In a recent case in Germany, attackers used Google AdWords to attract users who searched for “flash player” to the attacker’s fake Adobe-look-alike site. (*McAfee, “Web Browsers: An Emerging Platform Under Attack”*)

Criminal enterprise: In parallel, McAfee is seeing the growth and maturity of the online criminal enterprise in which consumers can be fooled into participating as “cybermules” *(“McAfee Virtual Criminology Report, Fall 2008”, Malware Grows 10-fold in 2008*). Using layers of criminals who specialize in specific roles within the criminal enterprise, risk is reduced. Some parties develop the software and sell it for use to steal information. Others steal the data (credit cards, stripe data, etc.) and re-sell it for fraud. Website operators agree to host malicious code for unsuspecting victims. Cybermules, who conduct money transfers – transferring money from one currency to another through “offline” wiring services - become easy scapegoats and are easily replaced with the next witting or unwitting participant to the trade.

Because of these and other realities to be discussed, there continues to be an *increase* in both individual consumer victims as well as the broader-impacting data breaches worldwide by the businesses and government agencies responsible for the protection of citizen, employee or customer data.

b) The implications of these risks on the wider economy, including the growing economic and security impact of botnets;

When it comes to botnets specifically, due to the continued lack of appropriate protection – or updates to that protection – on consumer machines, botnets will continue to succeed. In Q1 2009, McAfee detected nearly twelve million new IP addresses operating as “zombies,” computers under the control of spammers and others. This is a significant increase over the levels from the last quarter of 2008, with an increase of nearly 50 percent. (*McAfee Threats Report: First Quarter 2009*). Extensive botnets give hackers huge amounts of bandwidth, which they use for various illegal activities, and are responsible for the large volumes of spam messages that lead consumers to the malicious websites mentioned above. In fact, a single PC in a botnet can be used to send thousands of spam messages per day. Given this, botnets can continue to be a malicious cycle which feeds itself. When you consider that even one person who falls for one of the thousands of messages could stand to lose thousands of dollars, the risks to the economies of our country and world simply multiply. Botnets also assist cybercriminals in committing DDoS (distributed denial of service)



attacks against companies or organizations. This has several potentially damaging impacts to our economies – lose in business for the individual business, but also, if causing damage to a critical sector such as banking, transportation, or government, the economic impact could be enormous. As a result of their success, botnets are also a frequently traded commodity among spammers and attackers.

Obviously, the non-quantifiable costs are those in victim time and effort and emotional damage. The greater economic impact comes from not only the individual's loss of financial resources but those local resources from government agencies and businesses who must help re-establish credit histories, accounts, and identities. Costs to businesses can obviously be even more significant to the economy. In aggregate, revenue lost when individual citizens are defrauded from their life savings and retirement, can have a tremendous impact on a local economy. In the case of some victims in the U.S., families have lost entire retirement savings – tremendous cost to the family and tremendous costs to the local economy which would have enjoyed the benefits of such. (*Jamaican Scammers Threaten Minnesotans to Pay Up*, Stop H-Commerce).

Because it obviously takes significant resources to *fight* cybercrime, as it does physical crime, and to keep those who enforce *educated*, it is important to devise smarter, more efficient ways of sharing information to fight the cybercriminals, preserving resources as much as possible.

b) level of understanding and awareness of e-security risks within the Australian community;

McAfee applauds the efforts of the Australian government, AHTCC, AUSCERT and other organizations in their important role in helping Australia's businesses and consumers. We can and should work together to continue educational efforts, as in the National E-Security Awareness Week, to reach as many citizens and institutions as possible. Our global statistics of cybercrime victims – including identity theft and financial fraud – inform us all that we *must* continue and support these efforts. One important point is that most are likely unaware that they will become part of the problem when they choose *not* to leverage basic security protections on their devices. They make not only themselves, but those with whom they communicate, and millions more they do not know, if part of a bot network. While U.S. studies, the following figures are likely similar for most developed nations and can be informative for a strategy to protect Australia's citizens. They show that issues start with both consumer lack of appropriate protections as well as businesses who fail to protect the information in their care. In the consumer base, the McAfee/National Computer Security Association (NCSA) biennial study (October 2007) indicated:

- 78 percent of respondents do not have core protections

- 48 percent have expired anti-virus (even though 92 percent think their software is current) (Source:)

In the business-related issues impacting citizens and customers, attention to both the internal and external threat is important, as is a healthy attention to both inadvertent mistakes and lack of effective processes, and *intentional* data disclosures by insiders.

- A Dell/Ponemon study on laptop losses (June, 2008) indicated that business travelers lose *12,255* laptops per *week* in U.S. airports.
- >53% of business travelers say that their laptops contain confidential or sensitive information, while 65% of these travelers admit they do not take steps to protect or secure the information contained on their laptop. Coupled with trending provided by the U.S. Identity Theft Resource Center, in that country, the majority of businesses suffering breaches of information had no password or encryption protection on the data disclosed.

Obviously, there is much that can and should be done to help users understand basic best practices that benefit not only the individual user, but the community – and the world – at large.

c) measures currently deployed to mitigate e-security risks faced by Australian consumers;

I. education initiatives

In Australia, McAfee applauds the efforts of the government at all levels, the AHTCC, the banking industry, Service Providers, AUSCERT, and other in educating Australian consumers about online threats. Because they have such significant roles to play, all of these players together with organizations such as schools, retired community associations and facilities, and others can have a positive, and ongoing influence on the online behaviors of Australia's citizens. Specific examples of such systemic education includes but is certainly not limited to:

- Government
  - National E-Security Awareness Week
  - StaySmartOnline,
  - AHTCC's www.thinkuknow.org.au
- Financial institutions
  - ANZ Bank's "Protect Your Banking" (http://www.anz.com/aus/personal/ways-to-bank/internet-banking/protect-your-banking/default.asp)
  - Commonwealth Bank of Australia Security and Privacy info portal (http://www.commbank.com.au/security-privacy/)

  - National Australia Bank (NAB) security resources (http://www.nab.com.au/wps/wcm/connect/nab/nab/home/Personal_Finance/12/3/?ncID=ZBA)
- Service Providers
  - Telstra's BigPond Security Centre (http://my.bigpond.com/help/security/default.jsp)
  - Optus Personal Security Suite (http://personal.optus.com.au/web/ocaportal.portal?_nfpb=true&_pageLabel=Template_woRHS&FP=/personal/customerhelp/securitysuite&site=personal), Online Scanner and PC Health Check

Arguably a daunting task but finding ways to scale this knowledge so that it is *systemic* will be key to any ongoing awareness. Because education has to be intrinsic to our everyday lives, starting with our first PC or mobile device, there may be an opportunity for retailers, device manufacturers and the security industry to work together to provide 'get started' online driving materials for new PC purchases. Think of this as "driver education" for the online highway. We don't put people behind the steering wheel with driver's education. Yet we arm people with devices for internet access everyday, regardless of how versed they are on the dangers awaiting them. This education must include the fact that all of us who don't practice good "computer hygiene" are culpable parties to online crime. This is rarely pointed out to consumers so users do not make the connection that they are part of the *problem* – passing links, cute software on social networking sites, and emails onto others, easily becoming part of a bot network.

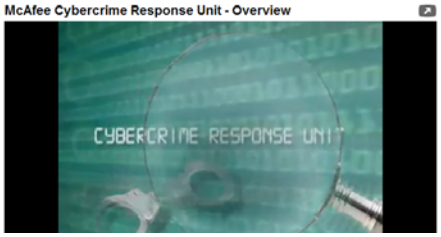
An important demographic in the educational initiative is the senior community. As in the physical realm, seniors are easily targeted and are not always armed with access to the information about internet risks. (*Jamaican Scammers Threaten Minnesotans to Pay Up*, *Stop H-Commerce*).

Free resources are particularly important to those who cannot afford access to software and training. One example is McAfee's Site Advisor which uses simple red/yellow/green rating to inform users of websites which could place them and their device in. While disparate sources are available today, succinct, aggregated portals of information for victim assistance in all forms of online crime is also necessary. This year, McAfee introduced an initiative known as the Cybercrime Response Unit (CRU) in the U.S. and anticipate expansion to the rest of world if

Learn more about the

Cybercrime Response Unit:

http://www.youtube.com/watch?v=mWPheSxY-1w


McAfee Cybercrime Response Unit - Overview

there is interest. An online portal for citizens to locate victim resources, regardless of the online crime, they also learn what puts them at highest risk, where to seek law enforcement assistance, and where to seek financial assistance for fraud. It includes tips on how to use social networking safely, and other information that is globally applicable.

II. legislative and regulatory initiatives

McAfee applauds the Government of Australia's activities across the Australasian Identity Crime Policing Strategy, the federal Privacy Act and its Privacy Principles, Australian Law Reform Commission (ALRC) work on data breach laws, and *this* initiative to protect citizens from cybercrime. We offer these considerations in the context of legislation and regulation.

- As we must in all areas of the world, it is important to regularly review and when necessary update the language in our laws to ensure all aspects of victim rights are afforded. Engage law enforcement to ensure that information flow and prosecution is facilitated through our laws. The newest laws should acknowledge and support the expeditious nature of the internet, and thus its crimes, ensuring that expeditious legal processes are ensured and supported (vs. awaiting a warrant to stop a cybercrime money transfer) in order to thwart further loss. Because our lives are online, crime is fast and so must our laws adapt to accommodate a swift response.
- If they exist, remove any monetary threshold (for damages) that act as impediments in the prosecution of online crimes, as was done in the U.S. in 2008 (the Identity Theft Enforcement and Restitution Act of H.R. 5938). But McAfee recommends coupling that with the appropriate resources to pursue these online crimes.
- Support resources for sharing information across jurisdictions so that similar crimes, perhaps perpetrated by same individuals with same tactics, can be readily identified. Aggregating such evidence could help yield greater prosecutorial penalties under existing laws. In cases in the U.S. where monetary damages are not immediately known, for example, agents use estimates for the virus removal services multiplied by the number of ip addresses involved in a botnet to prosecute the criminal responsible. Laws that do not sufficiently cover the online crime can sometimes use analogous laws applying to traditional crimes, or complementary laws such as those dealing with fraud, embezzlement, and theft when applicable and if possible.
- Encourage all businesses and government agencies to do their part so that less regulation is necessary. The use of best practices including employee training about web 2.0, vulnerability of mobile devices, and other issues of data

protection in their charge is critical. Ultimately, diligence and accountability should be a part of the business security fabric..

- As you've begun to do in the important work of the Australasian Identity Crime Policing Strategy, facilitate citizen assistance in rebuilding their financial lives and identities. It is commendable that you have already recognized the need to both facilitate the criminal pursuit, but to ease the process for victims with credit agencies, banks, driver's license agencies, and others who will necessitate proof of crime and help victims return to normalcy.

III. cross-portfolio and inter-jurisdictional coordinations

Again, McAfee applauds this important step in dialogue across public and private sectors. The public sector can have meaningful engagement with the parties who have the greatest impact on thwarting online crime or catching perpetrators. A candid dialogue acknowledging the role of domain name registrars, service providers, law enforcement, social networking providers, monetary wiring services and others in fighting cybercrime is key. *Ongoing* collaboration can facilitate the exchange of ideas in a swiftly-changing threat and online technology environment.

Determining processes that can facilitate information flow across these public and private sector constituents for successful investigations and arrests is also critical. The dialogue should include a frank discussion as to the *impediments* which prevent service providers and law enforcement, for example, from having meaningful, productive relationships in the pursuit of a crime. These frank discussions enable better, more effective laws.

Some challenges must still be faced to ensure that there is ease of information flow and resources across jurisdictions even *within the same country*. As an example, the U.S. still struggles with lack of a comprehensive, coordinated approach to cybercrime which normalizes the way all jurisdictions approach it. Some local jurisdictions are better resourced and more focused on online crime than others. In addition, while resources are available to help businesses victimized by online crime, individual citizens still get little assistance. Instituting processes to share information as addressed previously, could help ensure resources can be pooled and information can be expedited to help *all* victims and achieve higher success rates in catching cybercriminals before further damage ensues.

IV. international cooperation

We applaud Australia's many initiatives in fighting cybercrime including their participation in the Strategic Alliance Cyber Crime Working Group of international law enforcement partners, among others. While the

Convention on Cybercrime or similar frameworks can be sound models for normalizing our legal languages across borders, successful models facilitating information flow across borders have also helped lead to the successful location and arrest of cybercriminals across borders. Such models have included information sharing through co-located legal attaches, for example, (*FBI deploys cyberagents worldwide, Combating Cybercrime: Global Network Operates 24/7*) and it appears Australia is a part. Some examples of successful cross-border cases include:

- Romanian Cybercrime ring busted
- 'The Analyzer' Hack probe widens
- International phone hacking ring busted
- Kidnapped Hacker found in Turkey, arrested
- Jamaican Scammers Threaten Minnesotans to Pay Up

d) future initiatives to further mitigate the e-security risks to Australian internet users;

As indicated throughout this response, there are several areas in which future initiatives can help:

- forums to facilitate frank discussion both about impediments to inform legal language and processes, and to provide ongoing dialogue between public and private sectors to address swiftly-changing threats and provide swift responses;
- continued education/awareness campaigns that instill a sense of responsibility - that consumers themselves facilitate the spread of online crime and the need to follow basic best practices and good device "hygiene" (updated personal firewall protections and anti-virus updates). Having such educational efforts throughout everyday societal activities – shopping for computing devices, attending community events, and other societal activities – will lead to higher collective consciousness of the issues;
- education/awareness campaigns for businesses to diminish breaches, particularly those prevented by appropriate processes and already-available technologies
- support of resources to help victims and law enforcement.
- improved resources and training for law enforcement, with possibly specific career tracks and improved pay as incentive for specialized training may be worth consideration.

e) emerging technologies to combat these risks

Research, Innovation and today's evolving technologies for *protection*:
The security industry continues to improve technology solutions for better performance and less impact on our daily lives. This requires consistent

investment in Research and Development, and McAfee is committed to this. Given the industry challenge to keep endpoints updated with the very latest threat information in a rapidly changing threat environment, in 2008 McAfee began fully leveraging "cloud-computing" in the pursuit of faster time to protection. ***McAfee Artemis Technology*** dramatically reduces exposure from malware for which there is no current signature available. Millions of endpoints benefit directly from swifter decision-making from "in the cloud" community threat intelligence gathered by McAfee Avert Labs. Artemis-enabled end devices seamlessly send snapshots of suspicious files and in near real-time receive quick protection decisions rather than the traditional wait for the next scheduled update. The industry will continue to evolve its protections in this way so that customers benefit from faster time-to-protection and reduced performance implications. **McAfee's *Site Advisor*** is a powerful way to help inform users of the dangers of the web – for free - for safer web browsing and search. Our web security research has rated over 25 million sites, and McAfee has identified over 400,000 zombies identified per day.

Technology to enable *enforcement*: It is equally important that, as part of this dialogue, technology focus is not only for *protection* mechanisms. We must find ways – as the cybercriminals do – to improve communication within the community. Those on the front lines of enforcement need better tools and processes. Technology can help ease the burden to facilitate cooperative processes between law enforcement – across states and countries – and prosecutors, judges, service providers, and even money transfer agencies to share information leading to the demise of the criminal and the damages they inflict.

Use of evolving technology: Lest we place too much focus on technology, it is important to note the necessary balance between technology, the people, and the processes involved that:

a) better protect our machines and thus our lives,
b) enable law enforcement –regardless of jurisdiction or borders crossed, regardless of one individual victim or many - to track and reach the criminals, and
c) enable prosecutors and judges the *priority* and the *means* to prosecute the criminals.

A more protected community of users cannot stop with industry's research and innovation. As noted throughout this response, there are still significant gaps to address on the user side. Businesses *and* consumers still today don't use what is *already* readily available. They must use basic, *foundational* tools and implement them appropriately to get the full value from their use – lest any evolving technology be for naught. For example, consumer's purchase or use of free anti-virus tools does not end their responsibility to the security of their computing devices. They must be proactive in their updates and must maintain their subscriptions – free or paid. While technology continues to be *available* to protect, consumers and businesses must implement the free and paid tools available to them to inform their browsing habits. Because there is tremendous growth in the use of malicious websites, spam and other ways of luring users to those websites, users should be informed of the level of risk of each website in their search results and *act* with this knowledge in their browsing behaviors.

Still today, businesses and government agencies may not know about the personal data – employees, customers, citizens – they have, and where it is located. If the U.S. is any indication, the existence of laws and enhanced technologies does *not* mean businesses have increased their priority of protecting data where it needs to be protected – except for those who have learned first-hand of the brand and monetary damages such breaches cause. Paying attention to both the external threats but including those internal – inadvertent and malicious – threats from insiders is critical. Leveraging lessons from the U.S. may be helpful in informing what works and does not work in protecting Australia's citizens. Influence and education may be the greatest need indeed.

If all else fails, we may have difficult decisions to make – from placing liability entirely on consumers with unprotected devices, to an internet divided between "for fee" *trusted* vs. "free" *unvetted* internet. These may not be the *right* answers, but they *are* being considered on the global stage as possible ways to reduce cybercrime.

McAfee Inc.
McAfee believes that as technology providers, we must play a significant role in several areas:

- Education & awareness
  Given the above, we must continue to counsel businesses and consumers, in their own respective language to which they relate, of the basic processes they should follow. Using brand damage and other monetary losses to a business' bottom line vs. the theft of identity or financial impacts of fraud to individuals, we must find ways to make it 'real' *before* they become victims. Fundamental best practices do not generally change rapidly, regardless of the changing face of malware and cybercriminals' tactics. Best practices are readily available, and are included in McAfee's Cybercrime Response Unit portal.

- Research & Innovation – As noted, McAfee will continue to seek better, more streamlined ways of providing security while enhancing the level of security across our entire portfolio. But innovation does not stop there. We hope to continue dialogue with all of us who seek solutions to the world's online crime growth to understand what other important contributions we can all make by great dialogue among us.

About McAfee's Initiative to Fight Cybercrime

Based on the phenomenal growth in threats and online crime seen by our researchers worldwide, McAfee launched the Initiative to Fight Cybercrime in October 2008. McAfee's multi-point plan to fight cybercrime focuses on 3 areas of priority: *Education and Awareness*, *Policy & Legal influence*, and *Research & Technology*. Since McAfee launched the Initiative, we have provided grants to help educate prosecutors and judges worldwide about cybercrime, through grants to both the Council of Europe and the National District Attorneys Association. We also launched the Cybercrime Response Unit (CRU), a new online portal for consumers and small/medium businesses. The CRU provides education about online behaviors leading to higher risk of cybercrime, as well as links to the resources to report online crimes from crimes against children to intellectual property theft. In the way of policy and legal influence, our work with the Council of Europe hopes to encourage even more countries to become signatories and implement the foundation of the Convention on Cybercrime for easier prosecution across country borders. We continue to provide expertise in key policy and legislative reviews in Congress about everything from grants to local law enforcement in fighting cybercrime, to better legal language to improve *existing* and to implement *new* legislation. In the way of Research and Innovation, we introduced v1 of the free Cybercrime Scanner for the CRU which seeks to identity issue areas on a user's computer which make them vulnerable to cybercrime. Finally, a new cybercrime forum (http://cybercrimeforum.mcafee.com) implements a community in which our partners and associates in cybercrime can come to exchange ideas and work together in an online forum. Feel free to join the Forum, ask questions of the experts, and contribute your knowledge in this online community.

- Law: As technology evolves and new threats emerge, we must continue to ensure our cybercrime laws are ***modernized*** to match these threats (botnets is a good example); in the US, we have recently-passed legislation to do just that. Internationally, we must work to attain a level of uniformity among nations regarding cybercrime laws to prevent countries from becoming safe havens for cybercriminals. We must go beyond the current Council of Europe Convention signatories with more countries fully ratifying and and enacting this important treaty.
  - "We need an integrated legal framework to exchange data. A lot of legislation doesn't consider a data stream as evidence, because the evidence is hidden behind 0s and 1s. We have to rethink the legislative framework," – Bernhard Oputal, Interpol's Financial & High Tech Crime Division
  - "With phishing and pharming, new technologies are being dealt with by old laws," – Bernhard Oputal, Interpol's Financial & High Tech Crime Division
    - http://news.zdnet.co.uk/security/0,1000000189,39258540,00.htm
  - "Something has to be done about the breadth of the law as well as its vagueness. We need to pinpoint more details on what a cyber crime is and put a little more technicality in the law. If it's too vague, the hacker can just use that vagueness to his advantage. We need the law to be

more technical," - Ryan Flores, Team Leader of TrendLabs Phillipines, Speaking on Global Cyber Crime Law

  - http://newsbreak.com.ph/index.php?option=com_content&task=view&id=4894&Itemid=88889066

ISPs should be actively engaged to be part of the dialogue and part of the solution given their important oversight and responsibility for the traffic which flows through their networks.

In McAfee's part, we continue to use our gains in daily security research to inform governments worldwide of the dangers facing their citizens. We will continue to help our friends in law enforcement, in the consumer base, and in businesses have a voice in government as it relates to cybercrime and its impact on the greater society as it impacts each of these communities of interest.

Free McAfee resources available to you, your employees, your constituents

We hope that you can gain from the free resources available to help in this important endeavor.

McAfee resources include:

- McAfee Security Advice Center for families (http://home.mcafee.com/AdviceCenter/Default.aspx)
- HCommerce documentary (http://www.hcommerce.org/) for consumers
- For businesses, governments, and more technically-adept consumers:
  - McAfee Threat Center (http://www.mcafee.com/us/threat_center/default.asp)
  - McAfee Audio Parasitics podcasts (http://podcasts.mcafee.com/audioparasitics/)
  - McAfee Research blog (http://www.avertlabs.com/research/blog/)
  - Research reports and journals (http://www.mcafee.com/us/threat_center/white_paper.html)
    - Quarterly Security Journals
    - Annual Virtual Criminology Reports
    - Other topical research reports

McAfee's Global Threat Intelligence

From our base of our 100 million consumers and 50 million enterprise nodes, McAfee has an eye on the pulse of the threat environment. Our research includes the following reach:

- Web security research rating over 25 million sites, and over 400,000 zombies identified per *day*
- Malware research of 50,000 samples/day and 1.5 million malware detections in 2008 alone

- Vulnerability research of 100 sources daily and many new vulnerability discoveries
- Email security research of over 10 billion messages every month
- Network security research of over 10 million intrusion prevention alerts/day

From the endpoints where vulnerabilities can enter your network, to the protection of your critical or sensitive data in your care, to identifying policy violations to mitigate, McAfee has end-to-end solutions as well as security consultants in our professional services organization to help protect your organization and your data.