SUBMISSION NO. 1

MAY JUSTICE ALWAYS PREVAIL®

ABN:97144820620 GM-211-02C

PEOPLES POWER Reclaim our State and Federal constitutional and other legal rights, and hold politicians & judges accountable!

From; Mr. *G. H. Schorel-Hlavka,*
www.schorel-hlavka.com

Please note: WARNING ***The opinion(s) expressed in this letter by the writer, are stated considering the limited information available to him and may not be the same where further information were made available to him, is not intended and neither must be perceived to be legal advice!***

WITHOUT PREJUDICE

The Committee Secretary coms.reps@aph.gov.au 13-6-2009
House of Representatives Standing Committee on Communications
Suite R1-109, PO Box 6061, Parliament House Canberra ACT 2600
Http://www:aph.gov.au/coms

Submission Re Inquiry into Cyber Crime.

Sir/madam,

Cyber Crime is obviously a problem but worse to it is that many companies failto provide to have a system in place that ensures that at least they are not contributing to such kind of criminal activities.

Take for example where I received a few years ago countless email purporting to be from the Commonwealth Bank. The moment I received it I logged of the Internet (dial up) because the website of the Commonwealth Bank somehow didn't provide a scam notification section, and phoned the Commonwealth Bank about it. I was asked to fax a print out of the scam and also to email a copy to the email address they gave. I indicated I would phone later to check if they had taken action. About 12 hours later I contacted the Commonwealth Bank and after a long time on the phone it was made clear they had no knowledge of my complaint, my email or my fax, this even so I pointed out the times I had forwarded it from my own computer generated records. What this means is that while I was very concerned to seek to stop this Cyber Crime of scam emails regarding Commonwealth Bank (and considering I have no account with the Commonwealth Bank and hence immediately realised the notification about my account to be inactive if I didn't log in being a scam) nevertheless the Commonwealth Bank had failed any immediate action and so leaving its customers targeted with such a scam vulnerable.

In my view banks must have a clear (not hidden in all the text) section on its homepage to enable scam or suspected scam reporting as to seek to avoid customers being subjected to the scam where it can take action to prevent it.

Some years ago, I was receiving numerous emails having been rejected by an organisation as spam albeit I wasn't aware I had forwarded any of them. So, having received the rejections I found there was an email address on it and subsequently checking out which company owned this website I discovered it was an advertising company in the United Kingdom. I contacted this company and pointed out that they were using my trademarks **INSPECTOR-RIKATI®** and **MAY JUSTICE ALWAYS PREVAIL®** and requesting them to take action against anyone using my trademarks to promote their products as otherwise they could face legal consequences. I pointed out that by the High Court of Australia ***Gutnick*** decision the email having been received in the Commonwealth of Australia then were deemed to commit offences under Australian law and as such they could be prosecuted for this. After a few weeks I no longer received any rejects of emails and so the company clear had filtered through people promoting their products or the products of their clients to discontinue using my emails addresses which contained trademarks. Sure, they acted unlawfully in the first place to hijack my email addresses without my knowledge let alone consent but it is clear that I was able to achieve success in that regard. We then have to ask if I as an individual without the might of millions of dollars can achieve this then surely the Commonwealth Bank should have its resources available to take

immediate action to trace the senders of scam emails and take appropriate action against them. As a shareholder of the Commonwealth Bank I don't like it that shareholders and customers alike are loosing many millions of dollars because the Commonwealth Bank can't bother to have a system in place of immediate action against offenders. Below I have reproduced some recent scam emails which also relate to the Commonwealth Bank and indicate that for years it continues. Some days I get up to about 10 scam emails in a day just regarding the Commonwealth Bank! Obviously I get also scam emails about other banks from around the world and the problem is that not knowing which ones are genuine I simply delete all of them as spam even those of the bank I am with. This in turn results to a problem that where my bank does send out genuine emails I simply cannot take the risk to open it as if it is a scam I risk getting a virus into my computer. As such, the inaction of the banks against scammers has resulted that I refuse to open any emails from any bank, including my own bank!

.

Many banks are seeking customers to stop getting hardcopy bank statements and use Internet facilities instead but again with the risk of scam emails this is unwisely because if the bank were to forward any email I would delete it without opening it.

.

On Friday 12 June 2009 I received a phone-call from a woman who identified herself as **FRITZIE** claiming to be doing a customer survey for Dodo's. She asked if I consent to the call being recorded and I agreed to this. She then advises me that for security reasons she first have to establish who I am and so to provide my name, date of birth, address, etc. I refuse to provide the details as I made clear I do not know who she is and she can call me from anywhere in the world, etc. I asked her to make sure the tape recording is presented to Dodo management for it to take appropriate action. Well, I have been asking Dodo representatives each time over several months to do so but so far Dodo management have not responded. What this means is that Dodo management itself enhances CYBER CRIME because where it has this kind of system in place to ask customers their confidential details then when customers are used to this and get a (scam) email purporting to be from dodo then the customer wouldn't know better but it is from dodo.

.

I used to receive lost of emails from PayPal and Ebay about charges on my account even so I was then never with either of them. Since then I used both but the problem is that I cannot rust either of them because the avalanche of scam emails of both makes it extremely difficult to distinguish between which is not and which is scam email. Likewise was I getting up to 60 emails A DAY(!) scam emails about Yahoo, network solutions, etc. the result being I simply delete them all without checking its content because the moment one opens a scam email one risk a virus to get into the computer and I am not prepared to do so. And going through up to 60 emails a day all suspected scams is time consuming also and again not worth the risk. In the process it means that at times emails that are genuine may be deleted but then the risk outweigh this. For example the domain name "**OFFICE OF THE GUARDIAN**" was not extended due to the email being deleted and I found the **Centre of Human Rights** (NSW) then registering it on 19 may 2009 the day after they became aware of my 18 May 2009 email I was setting up the **OFFICE OF THE GUARDIAN**. As such, it was using public funding to snare various **OFFICE OF THE GUARDIAN** email addresses even so it clearly had nothing to do with them. As such it must be questioned why on earth the Centre of Human Rights took out various registrations if not for possible CYBER CRIME in the future. After all it may have done so to seek people wishing to contact the **OFFICE OF THE GUARDIAN** then to be redirected to the Centre of Human Rights (NSW) and so this in itself must be considered CYBER CRIME as people who in good faith search for **OFFICE OF THE GUARDIAN** are then ending up at the Centre of Human rights and as such misdirected. Cyber crime often commences as some small enterprise and when successful enlarges. I do not accept that the Centre of human rights should get involved in this kind of CYBER CRIME but so far it has failed/refused to reply upon my correspondences. One

may then ask as to the standing and integrity of the Centre of Human Rights (NSW) to get engaged into such kind of groundwork for cyber crime.

.

Many of the scam emails I receive have an Yahoo email address and are purportedly of Yahoo indicating it will close down my account if I do not verify my details such as password. Now surely Internet providers and other Internet companies such as Yahoo should never permit this kind of misuse of its identity going on? Surely Yahoo should have a filter system in place that the moment the word Yahoo is use it is checked for authenticity? After all where it purports to be an official email from Yahoo it should be entitled to check its authenticity?
And this is the same where it uses Yahoo email addresses there should be an immediate check.

.

On Friday 12 June 2009 I was seeking to post an article but instead of typing my email address with I accidentally typed this as I have also .com.au email addresses.
Still, when I pressed "submit" the immediate response was that the email address was invalid and I then corrected it. What however was shown to me was that somehow the media outlet (news.com.au) within a faction of a second had checked my email address and refused it for being not a valid email address because of the .au extension! If then a media outlet can detect this then surely other companies should be able to do likewise. Albeit it was a typing error in my case nevertheless it proved that it is possible to check email addresses as such.

.

On Friday 11 June 2009 somehow (as usual) my computer automatically updates programs and so did with Internet Explorer, which I didn't realise until 12 June 2009 when I got persistently a request to authorise access to my computer and it turns out to be internet explorer. I then discovered that due to an automatic update of internet explorer I now am pestered time and again with a request to permit access and in the process when I am spending time on the Internet in a certain program it gets cancelled out and so I have to start all over again. When I refuse to authorise the access then simply the Internet Explorer refuses to operate at all and so I am denied any Internet access. In my view this kind of terrorism shouldn't be permitted as it means that unless I allow access by internet explorer (and who knows what they do with the information) I am denied to use my computer for internet access. Now I have to try to fork out how on earth to disable the updates as to try to get back to the way it was.

.

Considering that I have at least 100 dial up connections (cost) in a month even so a month has about 30 days it means that on average I need to dial up 3 times a day because I get so often cut off the Internet sometimes after being less then a minute on the Internet!
How is this relevant to CYBER CRIME you may ask? Well, because I refuse ongoing updates and access not knowing who on earth wants access it means that I am getting off time and again. Now this is a very annoying matter when this happens at least about 70 times a month!
What it does mean that many getting frustrated by this may then just allow any access to their computer and then be subjected to CYBER CRIMES.

.

While my current computer is a recent one and has all the Internet virus protection, the previous computer was without it as I had disabled the lot because with the virus protection it could take up to about 5 minutes just to open an existing document. As a person who writes a lot and does open and close documents sitting idle time and again for up to 5 minutes just to open a document isn't what I wanted and while putting up with it for more then 6 months I finally got rid of the virus protection and now my documents come up without delay. As such, virus protection only is suitable if it doesn't cause this kind of unrealistic delays. Surely common sense should indicate that when you are off the Internet and still face up to 5 minutes delay for a virus check on past

created documents then this undermines the very virus protection system because people simply then delete the virus protection system as it is to much of a problem on its own.
The alternative now is to have just one computer on the Internet with virus protection and then transfer it later to any of my other computers. As such, initially any incoming material has a virus check but then can be used without having to re-check it time and again needlessly.. sure it is cumbersome to transfer it via USB stick but that is the best alternative.

.

When I used recently Bluetooth to wireless transfer material from one computer to another I suddenly discovered that my computer that normally goes on the Internet had lost its Internet facilities. I spend days trying to work out what was wrong and when I finally removed the Blue tooth system my computer re-instated its ordinary internal-modem. As such, while for a while there was no problem, suddenly there was a conflict and my internal computer modem program was annihilated. Take it from me that trying to work out the cause isn't a minor issue! Sure, I had still a laptop to go onto the Internet but try to find a solution is another thing and so I had to work it out for myself. With CYBER CRIME you cannot disregard this because on the Internet there are many programs available claiming to fix the problem of a lost modem program but dare to download it and my laptop might be infected with a virus in the first place and secondly the computer that gets the program likewise might be subjected to a virus. Hence, the risk to download such a program isn't worth it.
In the end a lot of patience and endurance to test and test different set ups did the job.

.

We also have the manufacturer supplied viruses.
Some 11 years ago I was discovering a virus on one of my computers. I had the habit then to write on the label of the 3½ floppy disk the date I first used the disk. A friend of mine provided me (a computer technician with a large telecommunication company) with a virus program but all it did was to shut down the computer the moment it started up because of the virus. My friend recommended to throw the computer out. I didn't. I then decided to check all my disk on another computer and going by date the moment I put the EXPERT (label designing program) into the comp0uter it shows it was infected. As such, I knew now that the virus had been introduced by the company supplied program. All other disk used since that date were infected but not the disk dated prior to it. Having the problem that the computer would not work with the virus program as it would detect the virus and immediately close it down, I therefore took the virus program apart on yet another computer and then in stages transferred it to the first infected computer. Once I had it on that computer I reassembled it and the computer immediately began to disinfect itself and I then closed it down. Even of switching of the power at the power outlet. When I restarted the computer the computer was clear of the virus and so its memory (due to the power shutdown). I then did the same trick on the other infected computer, which was caused to be infected by me to test it. My friend later made know that he actually had learned from me how to save computers, as his company would ordinary throw them out (Consider the loss of data also!)

.

The point is however that the virus had been introduced by an official (non-writable disk) from "EXPERT" label maker and as such a virus that was placed on the disk at manufacturing. The company never admitted liability but did provide replacement disk for the infected disk.

.

Obviously it is not known to me if the infection had been caused deliberately or not but it does indicate that companies that produce computer programs can have employees who may add a virus to their program without the knowledge or consent of the company and then the virus can allow Cyber Crime to commence, pending what the virus is for.

.

As complained about previously to the Prime Minister, even for my wife to check up on social Security information on its website, being general information and not being of any private

information, having 70 or more request to permit a cookie hardly is what the Federal government should have as part of its own website because it encourage people to allow cookies and once they get used to do it for social security information then they are likely to do likewise with others. While **Social Security** might like to know who visits which webpage nevertheless the problem is that customers who do not desire to facilitate this information then are denied to access public information on the website another thing if a person wishes to log on to access private details but surely it never should be permitted to generate some 70 or more cookies for a person just to access common details that are ordinary published by the Federal government in publications like "Seniors"! What we therefore have is that where the Federal government itself is guilty of putting people in a position of having to accept cookies or being denied even ordinary public information it therefore enhances people, in particular the elderly to accept cookies of everyone. My wife at 76 given by me the understanding NEVER EVER to accept cookies of anyone on the laptop by this is prevented to even check ordinary details on social security as it demands to allow cookies. Now, to me this undermines the very purpose of why the information is published in the first place, that is to provide information to the elderly! While the webmaster for social security seems to want to know which pages are accessed, surely this is utter and sheer nonsense when it comes to by this refusing access to web-pages . With my websites I have also that at time information might be asked, albeit not that I have set this yup for this, but anyone refusing to allow this still can access the web pages. It merely is for counting purposes (as I later discovered) but again anyone refusing to allow it still can access the web-pages.

Likewise I view social security should not prevent a person to access ordinary public information merely because the person doesn't allow cookies to be placed on his/her computer. In fact I counted at time 14 or 15 cookies request just to try to get onto the site before anything and as such it shows it is not just seeking to count because that would only take one cookie. Again management of social security replied to me that this is to know if the person still is on the webpage. Well, let me make clear that if I get some 11 or more cookies request one after the other within a space of about 10 seconds or less then this got nothing to do with trying to establish if a person is still on a webpage because I haven't even gone onto the page! As such the social security website is a gross abuser of the system and by this deny ordinary people the right of "public" information they are entitled upon to check. After all it is out in the open published in "seniors" and other printed information and as such not of a "personal private" content.

.

A few years ago I had a debt collecting agency pestering me about some $700.00 phone bill in regard of an address I did not own and neither ever had been. They demanded that I provided details but when I asked them the reason why they would respond something like that by the Privacy Act they were not permitted to disclose information, upon which I would respond that by the Privacy Act I neither could disclose information. After many months of this harassment and they even made clear to take me to court I made it clear to them that i9f they didn't desist in their conduct I would have them charged for STALKING, as within the legislative provisions it amounted to STALKING. Well, that did the trick. A year later another debt collection agency then tries the same and I made clear they better stop this rot or face the legal consequences. Well that was the end of them also.

.

And this is a real problem where companies like debt collectors are phoning without the person being called knowing the identity of the person and demanding to be given information. Like Dodo, one hasn't got a clue if the caller is genuine or not. Once you give out information it can be used for cyber crime!

.

I understand that A.G.E. purchased A.G.O. and by it got access to all closed accounts. Somehow then staff that have come over from A.G.O. used the old accounts to menace old customers through debt collectors that they still had outstanding accounts. Actually one of my son in laws

being a financial advisor had once a loan for a fridge and had this paid out years before the closing of the company but since the old records were transferred to A.G.E. he was subjected to harassment of debt collectors that he owned monies, albeit I understand A.G.E. itself denied any involvement. I understand a manager working for A.G.E. was working previously for the old company and as such access to the files and able to use his position at A.G.E. I understand also that accounts wro0ngly closed of prior to the sale, as to devalue the companies overall financial status, were later reverted albeit again I understand A.G.E. itself had no part of doing this and was unaware this was being done. What we therefore have is that cyber crime might be generated from ordinary transactions that took place years ago and then the old details on records can be used to commence cyber crimes because there appears to be no protection for past customers that their confidential information is not disclosed to others, including to the purchaser of the company long after the accounts were closed. Where in one case it involved an amount exceeding $160,000.00 one can hardly then hold that it are, so to say, peanuts!

Australia Post itself also is involved in this in that while the Framers of the Constitution did set up this combined federal system to serve the general public it now lacks any proper standing and integrity and far too many subcontractors are involved that undermine its security. For example three out of three parcels forwarded to the address of my grand daughter were never delivered but my daughter had to collect it from the post office, even so being at home to await the deliveries. (Formal complaints were filed and are on record to prove it!). We do however have Australia Post forwarding all kind of advertising material such as the Yellow envelope and as such it seems to be more concerned about making money then security. At one stage we had a $1,200.00 cheque (dividends) finally turning up when out neighbours returned from an overseas trip as it was in their mail box. Likewise legal documents turning up after 3-momnths having been somehow dumped somewhere else. Over the years I filed many complaints about failure of proper service.

While much might be argued about cyber crime commencing because people not having their mail secure and so others can steal it for identity theft and so also cyber crime, the truth is that Australia Post itself has recognised our post box is second to none and is adequate but the truth is that we have no proper mail deliveries and often even small envelopes are left hanging partly out of the mail box even so the mail box is further empty and is suitable for A4 size mail. As such, the lack of proper service by mail delivery personal is the real issue. With so many contractors, they do not want to get out of their vehicle either and so instead of loosing time to deliver a parcel to the door then rather just drop a card in the mail box that the parcel is to be collected from the post office. Many an elderly then have the problem of not only getting to a distant post office but then also having to drag a parcel home that should in the first place have been home delivered.

Cyber crimes are not just generated by theft of computers who are logged onto the Internet but also are the result of identity theft and other theft where Australia Post for example fails to ensure it delivers appropriately.

You have for example Centrelink demanding clients to provide statements of banking details, including amounts, bank numbers, branch numbers, et. A person can then personally deliver this to Centrelink to maintain as much as possible "CONFIDENTIALITY" well, next we knows that our neighbour receives our mail with all details in it because Centrelink send out statements making known that this is what they have on record and if it is incorrect to notify them. My 76 year old wife is furious that Centrelink is negligence in such manner to post out confidential banking details and then it end up in the hands of others, because Australia Post lacks reliable delivery. As such, any person who receives this kind of information can instigate cyber crime! With the millions of items of correspondences that Centrlink sent out it is obvious that many of the envelopes will be ending up in the wrong hands and so the issue is to avoid cyber crimes to

be generated from this by having Centrelink not sending out such complete information. I will not go into how they can do it differently as there is no need for this albeit sufficient to state it should not do so! In particular where a person seeking to keep it confidentially personally delivers the confidential details then nevertheless finds Centrelink posting it and it ending up in the wrong hands it underlines that cyber crimes can be generated at no fault of the victim but often the victim is unaware that their "CONFIDENTIAL" details were in an inappropriate manner provided to others to use it for CYBER CRIMES. While the police make known people not to leave mail for too long in mail boxes and make sure having secure mail boxes, this all is totally irrelevant where despite having appropriate mailbox facilities Australia Post leaves mail sticking out of the mailbox because the postman can't bother to get of his bike or otherwise deposit it properly in the mailbox or delivers it all together at the wrong address even so the mail address on the envelope is showing the correct mail address. My wife also made known to me that at times she was opening mail unbeknown it was not addressed to her, because it was between other mail delivered to her and then discovered details that were confidential of other persons. The real problem is that rather then Australia Post being as it was since federation it has been outsourced in franchises and so staff are mostly working for franchised post offices and not at all truly working for Australia Post. It is under the identity of Australia Post but that is all. When I lodge a complaint and get a response that the postman will be given training, then obviously I wonder why on earth this wasn't done in the first place with some person handling very important and confidential mail turning out not having been appropriately trained after all.

From personal experiences, when in management of a company, I made clear to my workers that if there was an issue then they should be aware I wanted to know about it. Hence, very often workers would alert me to matters knowing I wouldn't, so to say, bite their heads of, and in the process we had a considerable escalation of production because by being informed about possible problems I was able to address them before becoming major problems and so avoided loss of production and often resulting to an increase of production. Likewise, with Government Departments such as Australia Post and Centrelink (outsourced) if there was more alertness by the ministers (after all for this they are called "responsible minister" and be on top of issues that could become major problems then we would find a more safer environment for postal articles and other confidential details and by this lessen the risk of confidential information to be used for cyber crimes or for that other crimes. After all, the so called little old lady who may inadvertently have her bank details wrongly delivered and then have some perpetrator using this to rob her and perhaps kill her in the process, may all be avoided if just we had a better system of security and one that ought to be provided in the first place!

.

When then Australia Post sends out its Yellow Envelope with advertisements and this includes advertising of some fortune teller, even so during 2008 and before this so called fortune teller was exposed as a scam, then we have that Australia Post itself actually perpetuate cyber crime by trying to make money on advertising even so it advertises scams. Many of the elderly expecting Australia Post to be trustworthy then fall for this rot! Once they enter into some scam they are hooked for ever. I know because my wife was sending monies and now for years is pestered with correspondence for more! She too held that because it was provided by Australia Post then it surely was reliable, well she learned otherwise.

Cyber crime must not be deemed to relate just to identity theft of computers, as often the origin comes from non electronic sources, such as mail-outs of Australia Post.

Australia Post also has its on-line (Internet) survey and then spread this around to companies and so by this also enable to generate the basis for cyber crime. Again, I view Australia Post should not be involved in this kind of business!

I had ordered a parcel through an Internet based company but waiting for many weeks didn't receive it. I contacted the company and explained the dilemma. They promptly forwarded a replacement. We received the replacement as well as the original forwarded parcel together. I

presented the original parcel to the Post Office and asked them how much it would cost me to send it to the address (of the sender) and I was quoted about $10.00. Moment, I paid this company $5.00 for postage and handling and now Australia Post would charge me double just for postage? Sure, I could have forwarded back to "RETURN TO SENDER" but the issue was i wanted to check what Australia Post actually would charge me if I were to forward it in a normal manner, when I presented it in precisely the same condition (unopened) as it was received. As a **CONSTITUTIONALIST** I am well aware of the intentions of the Framers of the Constitution and one of them was that all people in the Commonwealth of Australia would have the same postal charges irrespective of where they lived. As I reside in Melbourne, the argument of perhaps living remote clearly isn't applicable either, not that it would be any excuse! The point is that Australia Post is charging me more then double for what it charges a company and to me this is a very serious matter. In my view its conduct is unconstitutional as it conflicts with the principles that are embedded in the Constitution, also it feeds cyber crime because rather then for example to post articles myself to family I might rather rely upon some company doing it for me by ordering it over the internet and then have the problem not knowing what is happening and making it more difficult to track it.

.

Getting back to for example the Commonwealth Bank scam emails I view that providers such as Yahoo should be well aware that these are spasm and indeed most of them are ending up in my spam box but somehow there appears to be no system in place that such suspected spasm are notified to the relevant banks. Meaning that people who are not suspecting it to be a scam may very well honestly respond with the consequences as result.

.

I may admit that about 8 years ago I fell for the scam and trying to get onto the website repeatedly using my identity and password it still wouldn't allow me to enter and it was then that I suspected it to be a scam and immediately gone the banks and cancelled all my cards making clear I suspected it to be a scam. It seems that due to my immediate action no harm was caused to my bank holdings. Still, the experience made it clear that it is easy to fall for a scam.

.

It has been reported that bogus bank websites are used (see below also) and surely Governments should be able to work together to make internet providers accountable for this kind of conduct. After all, the Framers of the Constitution, albeit living in a time of horse and cart were alert to the progress that could eventuate with telecommunication and for this provided in the constitution "**and other like services**" so as they held with progress of telecommunication the Commonwealth would have all needed legislative powers it may desire to implement.

While most people may hold that the Framers of the Constitution are long death and the Constitution is outdated the truth is the Constitution provided for the Commonwealth to legislate in regard of the Internet, etc. The Framers of the Constitution by using the wording "**and other like services**" foresaw the development albeit not to what extend and ensured no amendment of the constitution was needed to provide appropriate legislative powers.

Where then Internet providers and Internet based companies are operating within the sphere of the Commonwealth of Australia using telecommunication lines then also considering the HCA ***Gutnick*** decision I view the Commonwealth can legislate to hold companies using the Internet which is beamed/transmitted to the Commonwealth of Australia to be accountable for taking appropriate action against spam and spam users. As such, Yahoo, for example, should be facing its obligation to prevent scam/spam emails relating to Yahoo where it knows or should know that it is not official mail of itself even so it portrays to be so.

And, if the various governments were working together on this kind of system then cyber crime albeit not being a thing of the past surely could be severely reduced.

I view that Yahoo and other services who provide emails where it relates to the Commonwealth Bank or any other bank should be responsible that they ensure that the emails are checked as to

the email address authenticity being of the bank and failing this they are obligated to transfer the emails suspected of being scams to a relevant policing authority which then subject to an investigation may or may not forward it on to the intended person.

As much as I as an individual being able to stop some advertising company to misuse and abuse my trademarks then I view the Commonwealth Bank and other banks likewise could do the same. The question is however if the banks really don't care much about it as after all it are the shareholders and customers who are suffering the cost of the cyber crime losses?

.

I for one receive regularly scams about lotteries, including from The Netherlands. I took the time and effort to write to the Dutch Attorney-General who responded that it was not deemed to be a crime in The Netherlands. In my view this was wrong because where there is a participation of criminal activities with an address in The Netherlands then the crime is as much committed at the place monies are received as where the crime was executed upon an innocent person.

It is here that there is a lack of proper co-ordination between the governments and the failure to recognise that a crime committed in cyber space can only be committed if there is a actual crime being committed somewhere in a country. As such, the country where the email is generated is a point where a crime is committed. The country where the email is received is a point where the crime is committed. The point where the monies are received is a point where the crime is committed. As such there could be three or more points where the crime was committed in combination. It is therefore very essential that countries develop a policy that where their countries facilities, being it through the Internet, postal or other delivery services including any banking transmissions, involved their particular country then each such country has a legal position to prosecute those involved and where needed can cooperate with other law enforcement authorities to hold all those, regardless of the place or residence in the world, accountable. This to include freezing bank account of those suspected of participation, etc. Therefore, say the so called Russian mafia or the Nigerian scam is involved but they are seeking monies to be transferred to some third country then all countries involved can be deemed the scene of the crime and should be able to immediately take action to freeze assets, etc to prevent further transfer of monies to eventuate, etc.

I do get people complaining that I didn't respond to their emails but I make clear that I delete any suspect email and so unless they had some special indication to alert me it was not likely a scam I simply cannot take the risk. It is really terrible that this is how people have to safeguard themselves where I view appropriate legislation and obviously a proper working system could greatly diminish this cyber crime. The moment a scam email is detected and authorities are made aware of it and take urgent action to close it down the less likely such a scam can be worthwhile for the perpetrators. As such the issue is to ensure a proper working system is in place that can act immediately and not where a bank like the Commonwealth Bank despite my immediate notification some 12 hours later hadn't bothered to deal with the issue!

.

I now provide A Chapter 795 previously published by me in a book in the **INSPECTOR-RIKATI®** series on certain constitutional and other legal rights;

.

The following also need to be considered that laptops are available using finger print recognition to operate them and so limit usage to the holder of the fingerprint, as such more secure for the impaired in sight.

QUOTE Chapter 795

http://www.planetpapers.com/submitessay.php

WEBSITES DESIGNED FOR THE ELDERLY, BLIND, etc

Written by: inspector-rikati

When my wife at 75 for the first time in her life commenced a few days ago to log onto the Internet it appeared as if a new world had opened up to her. She took to it as a duck to water. . Now, a few days later, she is complaining that when she logs on she doesn't get immediately the right information but can have millions of web addresses to check out.

This in itself to her is a burdensome task and at her age she doesn't fancy to do so. . During the first attempt onto the internet I had allowed "COOKIES" to be downloaded on the laptop as not to confuse her in the initial learning, however for the second (HAVING REMOVED ALL COOKIES THAT HAD BEEN PREVIOUSLY AUTOMATICALLY DOWNLOADED) I then made the setting that she required to approve "COOKIES". Well, did this upset her. Over the years I had always explained to her the dangers of certain "COOKIES" and so when the screen flashed up about a "COOKIE" she really got worried. I explained to her to always refuse "COOKIES" no matter what she now does this.

Through the Prime Minister (Australia) was contacted about a complaint I had made regarding one Government organ seeking to download at least 76 "COOKIES" just to be able to enter its website. As such, there is a gross abuse of the system in that regard. The person who contacted me claimed not to understand why "COOKIES" were to try to download other then 12 different "cookies' were existing and needed to be renewed during a session. I pointed out that getting 76 "COOKIES" attempts to download just to try to enter a government website is absurd.

What is a shame is that my wife finally attempts to get involved with the computer age and then is bombarded with "COOKIES" which really have little purpose to what she is after. . Personally I have little problems with "cookies" because I use the internet for certain purposes, but surely we should have less inquisitive conduct by companies and government organisations by making websites more user-friendly and certain avoid a avalanche of "COOKIES" request to be downloaded. Once you refuse it that should be the end of it. While I do a permanent ban on "COOKIES" as to avoid being pestered with them, my wife however going on the Internet to search for information is bombarded at each web address with "COOKIES" request and even when obstructing the download still can enter the website. As such those who set up the website are really undermining attracting prospective customers by their absurd overuse of "COOKIES". Various companies I contacted never even realised that the business that did set up their website did associate "COOKIES" with it as it was to them no use, as they did not desire to know any such information. . Perhaps "COOKIES" free websites should have this indicated, so people who desire to be without a bombardment of "COOKIES" would be more likely be attracted to those websites. . A problem with "COOKIES" is that it may but may not seek to be used to trace what you are doing and/or obtain your personal information. Now, perhaps "COOKIES" that are needed for no more but strict verification of using a particular website (banking, personal blogs, posting under once identity in a web page like "Planet papers") should rename their "COOKIES" for this as "PERSONAL INFORMATION VERIFICATION COOKIES" so that the user knows what the "COOKIE" is to be used for, while then other "COOKIES" can be blocked, if one desire to do so.

Also, there should be a way of a person wanting to read the fine print this can be enlarged without the risk of accidentally downloading a "COOKIE". As my wife indicates she has really problems to read the "fine print" and so what would be needed is that in the task bar there is an option to say increase in percentage the screen so that the elderly can navigate around the page to see it all in a letter type they can read. The magnifying glass provision for enlarging certain pictures in certain programs could be used in that regard to enlarge the entire website on the screen, so the elderly (who have vision problems) can read it also. . Once one introduce a ability to enlarge the view on the screen, then when one allows this to be transferred to a remove screen useful for the partial blinds as a Braille touch screen (sensor pad), then a lot more people can

utilise the internet. Because those who are blind may not know when to touch a screen or not, it would then be better for them to have a "Braille sensor pad" that cannot be activated unless the person press a specific button for this. It would mean that a blind person could harmlessly search the Internet without any risk of activating anything and when desiring to do so then uses the button that specifically provide for this. In my view Braille sensor pad should be no difficulty to be created for this purpose. . As for "COOKIES", as they block generally any further use of the computer it would be better if they are required to be designed to be user friendly so that the vision impaired will have no problem to get rid of them.

User Comments

http://www.planetpapers.com/Assets/6818.php

WEBSITES DESIGNED FOR THE ELDERLY, BLIND, etc

When my wife at 75 for the first time in her life commenced a few days ago to log onto the Internet it appeared as if a new world had opened up to her. She took to it as a duck to water.

.

Now, a few days later, she is complaining that when she logs on she doesn't get immediately the right information but can have millions of web addresses to check out.

This in itself to her is a burdensome task and at her age she doesn't fancy to do so.

.

During the first attempt onto the internet I had allowed "COOKIES" to be downloaded on the laptop as not to confuse her in the initial learning, however for the second (HAVING REMOVED ALL COOKIES THAT HAD BEEN PREVIOUSLY AUTOMATICALLY DOWNLOADED) I then made the setting that she required to approve "COOKIES". Well, did this upset her. Over the years I had always explained to her the dangers of certain "COOKIES" and so when the screen flashed up about a "COOKIE" she really got worried. I explained to her to always refuse "COOKIES" no matter what she now does this.

Through the Prime Minister (Australia) was contacted about a complaint I had made regarding one Government organ seeking to download at least 76 "COOKIES" just to be able to enter its website. As such, there is a gross abuse of the system in that regard. The person who contacted me claimed not to understand why "COOKIES" were to try to download other then 12 different "cookies' were existing and needed to be renewed during a session. I pointed out that getting 76 "COOKIES" attempts to download just to try to enter a government website is absurd.

What is a shame is that my wife finally attempts to get involved with the computer age and then is bombarded with "COOKIES" which really have little purpose to what she is after.

.

Personally I have little problems with "cookies" because I use the internet for certain purposes, but surely we should have less inquisitive conduct by companies and government organisations by making websites more user-friendly and certain avoid a avalanche of "COOKIES" request to be downloaded. Once you refuse it that should be the end of it.
While I do a permanent ban on "COOKIES" as to avoid being pestered with them, my wife however going on the Internet to search for information is bombarded at each web address with "COOKIES" request and even when obstructing the download still can enter the website. As

such those who set up the website are really undermining attracting prospective customers by their absurd overuse of "COOKIES". Various companies I contacted never even realised that the business that did set up their website did associate "COOKIES" with it as it was to them no use, as they did not desire to know any such information.

.

Perhaps "COOKIES" free websites should have this indicated, so people who desire to be without a bombardment of "COOKIES" would be more likely be attracted to those websites.

.

A problem with "COOKIES" is that it may but may not seek to be used to trace what you are doing and/or obtain your personal information. Now, perhaps "COOKIES" that are needed for no more but strict verification of using a particular website (banking, personal blogs, posting under once identity in a web page like "Planet papers") should rename their "COOKIES" for this as "PERSONAL INFORMATION VERIFICATION COOKIES" so that the user knows what the "COOKIE" is to be used for, while then other "COOKIES" can be blocked, if one desire to do so.

Also, there should be a way of a person wanting to read the fine print this can be enlarged without the risk of accidentally downloading a "COOKIE". As my wife indicates she has really problems to read the "fine print" and so what would be needed is that in the task bar there is an option to say increase in percentage the screen so that the elderly can navigate around the page to see it all in a letter type they can read.
The magnifying glass provision for enlarging certain pictures in certain programs could be used in that regard to enlarge the entire website on the screen, so the elderly (who have vision problems) can read it also.

.

Once one introduce a ability to enlarge the view on the screen, then when one allows this to be transferred to a remove screen useful for the partial blinds as a Braille touch screen (sensor pad), then a lot more people can utilise the internet.
Because those who are blind may not know when to touch a screen or not, it would then be better for them to have a "Braille sensor pad" that cannot be activated unless the person press a specific button for this. It would mean that a blind person could harmlessly search the Internet without any risk of activating anything and when desiring to do so then uses the button that specifically provide for this.
In my view Braille sensor pad should be no difficulty to be created for this purpose.

.

As for "COOKIES' , as they block generally any further use of the computer it would be better if they are required to be designed to be user friendly so that the vision impaired will have no problem to get rid of them.

Thankyou! your essay has been added to the site and is available now at http://www.planetpapers.com/Assets/6818.php. It will also be listed on the What's New page for the next week.

If you would like to make changes to your essay you can do so by visiting the Edit Essay page

If you think your essay belongs in more than one category, please drop me a line and I will put it in the relevant categories

Submit another essay

END QUOTE Chapter 795

.

I now provide some of the scam emails to elicit details, etc;

QUOTE 22-6-2007 email
http://www.au.sorbs.net/cgi-bin/db
Database of servers sending to spamtrap addresses
Netblock:
Record Created: Thu Mar 30 11:46:28 2006 GMT
Record Updated: Wed Mar 7 16:20:17 2007 GMT

Additional Information:

Currently active and flagged to be published in DNS
If you wish to request a delisting please do so through the Support System.

This page was written to render correctly in any standards compliant browser, like Mozilla.
This link is provided for address collecting robots. Source code is here.

[Doc Id:
Getting Support From SORBS
Use the following sections for requesting support from SORBS. Each section explains common questions and their answers.

Please use the information to log tickets within the SORBS support system, as this will help the SORBS support personnel to assist you with your problem quickly.

For zone transfer requests please click here.

Note: This script is new and there are a couple of errors still, if you find them please report them to indicating what you typed and clicked to get to the error.

A few questions first.
To help us deal with your problem quickly please fill out the following form:

Note: Logging in will skip these questions.

What is your name (Format: First Last):
What is your email address *(required)*:

Do you need help or support about a listing, delisting, or blocked IP address?
yes Yes
no No
clue Not Sure

What OS do you use Primarily?
unix Unix (Solaris, Linux, HPUX etc)

	windows Windows osx Mac OS X mac Mac (pre OS X) clue Not Sure other Other (specify):
What is your skill level with computers?	clueless None, I can play games though. luser A little, just use them for email. normal Average, familiar with them, used at home and work. admin A lot, sysadmin or MCSE etc. guru My Name is Charles Babbage, or Alan Turing.
Are you requesting help for:	person Yourself company Your Company isp Yourself as you are an ISP na Does Not Apply

Note: ISP's if you are logging a ticket for a DUHL listing **and** the rDNS is set to something which we know your naming convention, or it contains one of the 'static' naming conventions like in the Suggested Generic Naming Schemes Draft RFC check 'Yourself' and enter one of the listed IP addresses per /24 sized block. This will route any created ticket to the robot handler which will process and delist the netblock (upto /24) within a few hours, this is faster than routing the ticket to the ISP Support queue which can take a day or two.

1	Continue	Reset Form

END QUOTE 22-6-2007 email

.

QUOTE

Yahoo! Alert	***Important Information Regarding Your yahoo Account***	1:18 PM	4KB

Important Information Regarding Your yahoo Account
Friday, 12 June, 2009 1:18 PM
From:
"Yahoo! Alert" <alert@yahoo-inc.com>
To:
undisclosed-recipients

Dear User,

We are sorry to inform you that we are currently working on securing our server, during this process account which is not manually verified by us will be deleted, Please confirm and submit your information for manual verification by one of our customer care.

Information which is to be provided is below:
User Name:
User Id:
Password:
Date Of Birth:
Country (At Sign up):

Upon confirmation of information from you, we will manually verify your Yahoo! Account and reserve it not to be deleted, We are sorry for any inconveniences this might have cause providing your information over the email.

Warning!!! Account owner that refuses to update his/her account after two weeks of receiving this warning will lose his or her account permanently.

NOTICE: We collect personal information on this site.

To learn more about how we use your information, see our Privacy Policy.

END QUOTE
.
FROM DR.KARIM BUSINESS CONTRACT AWAITING REPLY?
Friday, 12 June, 2009 9:35 AM
From:

To:
undisclosed-recipients

FROM THE OFFICE OF

WEST AFRICA

DEAR FRIEND
I KNOW THAT THIS MESSAGE WILL COME TO YOU AS A SURPRISE. I AM THE BILL AND EXCHANGE MANAGER IN BANK OF AFRICA (B.O.A), OUAGADOUGOU BURKINA FASO. I HOPED THAT YOU WILL NOT EXPOSE OR BETRAY THIS TRUST AND CONFIDENT THAT I AM ABOUT TO REPOSE ON YOU FOR THE MUTUAL BENEFIT OF OUR FAMILIES.

I NEED YOUR URGENT ASSISTANCE IN TRANSFERRING THE SUM OF (USD$15)

MILLION TO YOUR ACCOUNT WITHIN 10 TO 14 BANKING DAYS. THIS MONEY HAS BEEN DORMANT FOR YEARS IN OUR BANK WITHOUT CLAIM. I WANT THE BANK TO RELEASE THE MONEY TO YOU AS THE NEAREST PERSON TO OUR DECEASED CUSTOMER (THE OWNER OF THE ACCOUNT) DIED ALONG WITH HIS SUPPOSED NEXT OF KIN IN AN AIR CRASH SINCE JULY, 2000.

I DON'T WANT THE MONEY TO GO INTO OUR BANK TREASURER ACCOUNT AS AN ABANDONED FUND. SO THIS IS THE REASON WHY I CONTACTED YOU SO THAT THE BANK CAN RELEASE THE MONEY TO YOU AS THE NEXT OF KIN TO THE DECEASED CUSTOMER. PLEASE I WOULD LIKE YOU TO KEEP THIS PROPOSAL AS A TOP SECRET AND DELETE IT IF YOU ARE NOT INTERESTED.

UPON RECEIPT OF YOUR REPLY, I WILL GIVE YOU FULL DETAILS ON HOW THE BUSINESS WILL BE EXECUTED AND ALSO NOTE THAT YOU WILL HAVE 35% OF THE ABOVE MENTIONED SUM IF YOU AGREE TO HANDLE THIS BUSINESS WITH ME? AND 10% WILL BE SET ASIDE FOR ANY EXPENSES THAT WARRANT ON THE PROCESS BEFORE THE FUND GET INTO YOUR BANK ACCOUNT SUCH AS TELEPHONE CALLS BILLS (ETC).

BEST REGARD.

TEL CALL ME

END QUOTE

.

QUOTE
Scheduled Payments Notice
Friday, 12 June, 2009 11:27 AM
From:
"St George InternetBanking" <payments@stgeorgebank.com.au>
To:
undisclosed-recipients

Dear Customer,

St.George Bank has temporarily suspended your payments via BPAY View® .
Reason: Bills Online via BPAY View® failure
You are required to complete an account update form so we can unlock your account.

To start the update process click here.

Once you have completed the process, we will send you an email notifying that your account is available again. After that you can access your account at any time.

The information provided will be treated in confidence and stored in our secure database.
If you fail to provide the required information your account will be automatically suspended from Scheduled Payments database.

END QUOTE

.

QUOTE
Important Information Regarding Your Account
Friday, 12 June, 2009 5:29 AM

From:
"Commonwealth Bank" <accstat@news.com.au>
To:
undisclosed-recipients

Dear **Commonwealth Bank®** member,

We are happy to announce you that MasterCard has recently issued a security update for their clients in Australia.

With this update cardholders are protected by MasterCard's Zero Liability policy.
If someone makes an unauthorized purchase using your MasterCard, you will NOT be responsible for that purchase and the money will be returned to your account.

Commonwealth Bank advises ALL its clients to enroll their MasterCards for this FREE OF CHARGE security update.

Internet Banking: Enroll for the MasterCard security update

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,
Commonwealth Bank Security Department

END QUOTE

.

QUOTE
Important Information Regarding Your Account
Friday, 12 June, 2009 11:14 AM
From:
"Commonwealth Bank" <accstat@news.com.au>
To:
undisclosed-recipients

Dear **Commonwealth Bank®** member,

We are happy to announce you that MasterCard has recently issued a security update for their clients in Australia.

With this update cardholders are protected by MasterCard's Zero Liability policy.
If someone makes an unauthorized purchase using your MasterCard, you will NOT be responsible for that purchase and the money will be returned to your account.

Commonwealth Bank advises ALL its clients to enroll their MasterCards for this FREE OF CHARGE security update.

Internet Banking: Enroll for the MasterCard security update

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,
Commonwealth Bank Security Department

Commonwealth Bank of Australia 2009

END QUOTE

.

QUOTE
Dear Member - Commonwealth Bank of Australia [MESSAGE]
Friday, 12 June, 2009 10:38 AM
From:
"Commonwealth Bank of Australia" <secureonlinecomm@yahoo.com>
To:
undisclosed-recipients
END QUOTE

.

"Commonwealth Bank" <accstat@news.com.au> uses hyperlink;
"http://thecouvein.inthecouve.org/comwealth-mcd-update.html"
"St George InternetBanking" <payments@stgeorgebank.com.au> uses hyperlink: http://65-121-9-235.dia.static.qwest.net/redirect.php
Then we have the usage of yahoo as a bank email base!
"Commonwealth Bank of Australia" <secureonlinecomm@yahoo.com>, the problem with "St George InternetBanking" <payments@stgeorgebank.com.au> is that ordinary it would be extremely difficult to notice anything wrong with the Internet address merely looking at it.
What I view should be done is to prohibit Internet providers and companies providing email addresses to use email addresses which are deceptive or may be used for deceptive purposes.
As such the usage of "stgeorgebank.com.au" should have been deemed unacceptable as it purports to include a bank.

.

This submission is not intended and neither must be perceived to set out all issues of concern but at least gives some indication that the commonwealth has the legislative powers but the question is will it act appropriately for the sake of the general community?

.

Awaiting your response, ...Signature **G. H. Schorel-Hlavka**