Submission to the Standing Committee on Legal and Constitutional Affairs Inquiry into crime in the community: victims, offenders, and fear of crime

Small Business Internet Related Crimes or Adverse Activities

1 Preamble

I wish to bring to the Committee's attention a matter that has adversely affected, and could further adversely affect, businesses (in particular small businesses), their owners and current and former staff. The matter is that current Federal legislation and regulations do not ensure that the owners of company or business names can have their lawfully approved names as domain names. This has enabled a self-regulated party, the Australian Domain Name Administration (auDA), to establish policies that could lead to a company or business losing its lawful name as its domain name. That is, the lawful name of one business could be awarded by auDA to another business to use as its domain name.

This situation could lead to several internet related crimes or adverse activities that need to be prevented. Once a crime has happened the victim is a victim for life and it is then too late to recover the situation. Any sympathy, assuming it was provided, would be of little comfort to the business, and its employees, that were left with no practical option other than to close down. With an estimated 1.2 million small businesses employing about 3.2 million people, even a modest crime rate would have significant community implications.

The case study for the submission is a hypothetical small business called Tool Drool. However, the situations described below are happening to small businesses right now. It could easily happen to many more small businesses, and many of them do not know that they have this problem - yet.

2 Case Study

Tool Drool was established as a specialist tool business before the internet was a commercial reality, and has traded continuously ever since. Over time it has become a well know supplier of tools with a lot of goodwill attached to its name. Aware of the internet and its application, Tool Drool has not seen the need to get involved at this stage. Although it sees that this could change in the future.

The business is now a candidate for situations that could force it to shut down.

2.1 Situation 1.

A major warehouse chain (XYZ Pty Ltd) has noticed that Tool Drool is affecting its business and has a clientele that it would like to have. XYZ registers a business name XYZ Tool Drool Hire. The name is significantly different to Tool Drool and would be registered. XYZ Tool Drool Hire can then apply for, and would be granted, the domain name www.tooldrool.com.au.

XYZ Pty Ltd has now denied Tool Drool an opportunity to use its established business name as its domain name to develop its business on the internet.

The comments by Justice Anderson of the New Zealand High Court in the Qantas cybersquatting case seem analogous, at least.

http://www.qantas.com.au/regions/dyn/au/publicaffairs/details?ArticleID=1999/dec99/6293

To quote from the Qantas article:

> Justice Anderson said: "… the deliberate blocking of the lawful exploitation of goodwill by Qantas through registration effectuated for that purpose or with that consequence is a fraudulent appropriation of part of the goodwill attaching to [the Qantas] name.
>
> "The most likely purpose in registering the name of such a well known entity is to block that entity's lawful exploitation of its goodwill through the use of the internet.
>
> "It is important to appreciate, of course, that the domain name is the gateway to exploitation and the defendant's registration has blocked the gate. Such registration is … an instrument of fraud."

Any small business that is viable is well known otherwise it would not be viable. A business does not have to be a household name to be "well known".

XYZ Pty Ltd can then create email addresses for each of the current, future or former staff members of Tool Drool. XYZ Pty Ltd is then in a position to attract any internet based business that could be meant for Tool Drool, also, it can capture any email traffic intended for the staff of Tool Drool.

Tool Drool is now facing extreme risk levels (as defined by AS/NZS 4360 Risk Management) in terms of:

- Passing off
- Identity theft, fraud or compromise
- Privacy violations for the company and its staff
- Behaviour by XYZ Pty Ltd adversely affecting the business

As a small business it is probably not in any position to defend itself legally of competitively. The most likely option open to Tool Drool is to shut down and start up under another name or leave the industry all together. The financial and social impact on the owners and staff of Tool Drool should be obvious.

2.2 Situation 2.

A small work wear manufacturer business called Tool and Drool Workwear started in another state. Totally unaware of the existing Tool Drool business and by chance applied for the domain name www.tooldrool.com.au. Again, there is no reason why it would not be approved. Tool Drool has been denied the opportunity to use its established business name as its domain name. In this case there is no likelihood of passing off, unless of course the workwear company decided to get into the tool business. However, there would be identity compromise and an increased risk of privacy violations of the Tool Drool staff. There is also the risk of any adverse behaviour of Tool and Drool Workwear that might be reflected on Tool Drool.

2.3 Situation 3

A XXXX rated adult shop registers the business name Tooling and Drooling. It could apply for and would be granted the domain name www.tooldrool.com.au. Not only does it prevent the business with that exact name having its name as its domain name, it would create an obvious adverse impression and Tool Drool forced to close down.

2.4 Situation 4

A hobby business called Hobby and Model Drool Center has a major business segment in hobby tools. Although a little less clear, under current policy it is possible that it could convince a domain name registrar that due to the volume of its hobby tool business and the word "drool" appearing in its name, that it should be given the domain name www.tooldrool.com.au.

There are many other combinations that could be used to deny the name or even cause some confusion. All of these cases are to the detriment of the established business named Tool Drool.

3 The types of crimes committed against Australians

The possible crimes or other adverse activities that could lead to the demise of an otherwise viable business, and the consequential impact on its staff, are:

- Passing off
- Identity theft, fraud or compromise
- Privacy violations for the company and its current and former staff
- Behaviour of another company adversely affecting the business

These should be logically obvious and are based on current experience and legal or professional advice.

A more comprehensive discussion on the types of crimes is addressed in the following report. This is a much higher level document; however, it does provide a discussion on the frameworks that could result on the crimes or other adverse activities.

The Confederation of Asian and Pacific Accountants (CAPA) covering some 21 countries in the Asia-Pacific Region commissioned the Australian Institute of Criminology (AIC) to undertake a study on internet fraud. This report issued in October 2001 is titled "Controlling Fraud on the Internet: A CAPA Perspective" can be found at:

http://www.aic.gov.au/publications/whatsnew.html Publication 39.

This 130+ page report comprehensively describes the many and various forms of internet related fraud. For anyone interested in the subject, this is a "must read". It is well researched and documented and should be a mandatory reference point for anyone involved in developing internet based policies, or strategies to prevent or otherwise combat internet related crimes.

The Executive Summary # 3 (p1) defines internet fraud as:

> "Any act of dishonesty or deception carried out through the use of the internet, or directed at technologies that support the internet."

Executive Summary # 38 (p8) states in the conclusions that:

> "The continuing expansion of electronic commerce in business and government will create many new opportunities for those intent on gaining a financial advantage improperly by deception."

Paragraph 4.3.4 (p51) headed "Identity Related Fraud" states:

> "One of the most frequently used strategies to perpetuate fraud is the creation of false documents for misrepresenting one's identity."
>
> "The technology of the internet makes it relatively simple to disguise one's identity"

Further, the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce can be found at:

http://www.accc.gov.au/ecomm/CPGuidelines_final.pdf

Part II, Section II states:

> "Businesses should not make any representation, or omission, or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair."

A view often stated is that if the two companies are in different business sectors then there can be no confusion to the consumer if the domain name of one company is the same as the trading name of another company. Put aside the obvious lack of common sense of such a view. Even if the two businesses are currently in different business sectors, will they stay that way? To use the business sector assumption to justify the policy imposes a double jeopardy on both companies. In the case of Situation 2, by moving out of their current business sector they could infringe the pre-established identity of the other company and are then open to passing-off claims. If they can't move to avoid this situation are they then able to claim the lack of Government legislation or regulation as well as domain name policy is effectively a restraint of trade?

4 Perpetrators of crime and motives

The lack of legislation or regulations is an open door to a wide range of adverse activities.

In today's environment, given the issues such as terrorism, customs, immigration, taxation, security, pornography, etc it is hard to understand why a Government could even tolerate a known situation to exist where there could be any possible confusion over identities for the "bad guys" to consider exploiting. Instead of taking an arms-length approach to see what happens, Government should be taking extraordinary steps to make sure that any possible confusion or risks between the identification of two or more entities should not be higher than before the introduction of the internet. That is, the risks introduced by domain name policy should not be higher than accepted through either the Trade Practices Act or company name or business name approval rules.

There seems to be a concept that two companies can coexist with shared identical identities. One of then main reasons we have the A.C.N. system is because it was found that this did not work. Only an altruist without any business experience at all would hold the view that Business A wanted the lawful name of Business B as the domain name for A on a peaceful co-existence basis. This should be seen for what it really is: The intention of Business A to assume the identity of Business B and eliminate it. That is, the premeditated intent is cybersquatting or identity theft in one of its many camouflages.

5 Fear of crime in the community

The situation puts many small business in the nightmare grade crime prevention problem: i.e To stop a predatory company stealing your business name or identity. The protection of name and identity is critical to any small business as it is often the sole basis of their growth and livelihood. Whenever there is an encroachment of a small business name or identity it usually results in irrecoverable adverse outcomes.

The threat to a business name or identity is one of the issues most feared by small business.

6 Strategies to support victims and reduce crime

The simplest solution is for the Government to either legislate or regulate to protect the rights of a company to its name in any business context. There is a precedence for this as the Government regulated to protect the name of Sir Donald Bradman.

The solution is simple, common sense and obvious: A company/business that is continuously current on the ASIC register has exclusive first rights to that exact name as its domain name.

If a business wants a name other than its lawful name to promote its business on the internet then have a set of rules to do that; but no individual or business should have the right to a domain name that is exactly the same as the existing established lawful name of another business.

With the rapid increase in internet based crimes, small business is continuously being advised to have proactive business crime prevention methods in place. How can a business prevent

internet based crimes against it when the very policy to provide the gateway to the business, its name, actually denies a company from taking the most basic preventive measure: control the access to its identity? What is even more bewildering is that the Federal Government is on the sideline condoning a process where the outcome can only be described as legitimised cybersquatting.

Domain name policy and its implementation must not allow the situation to be a possibility, let alone exist, where a company's name could given to another company as its domain name. It is not a matter of law; it is common sense. It is time to set the idealism aside. A proactive internet crime prevention culture should be the basis of Federal Government domain name policy.

7 Apprehension rates

Given the convoluted legal issues involved, apprehension may not take place at all because it is often outside of the resources of a small business to take the necessary action. It may be easier for a small business to withdraw rather than engage in the time and legal expense of seeking independent justice. auDA is putting in place a dispute resolution process. However, it still carries with it the perception that as it is an auDA process it may not be as independent as a more transparent alternative commercial dispute resolution process.

8 Effectiveness of sentencing

No comment

9 Community safety and policing

The key community issue is protection of the identity of an employee of a business. There are many well-published cases of stolen identities that have lead to a complete life-long destruction of the victim. A small business can be a victim of crime similar to an individual. That is, its identity can be stolen and used to incur debts and other representational issues. It actually raises a very interesting issue about the liability of an employer to protect its current and former staff. What is the situation if the identity of an employee is compromised to the disadvantage of that person; are the owner's of the business liable?

10 Conclusion

To prevent a range of internet based crimes or other adverse activities that are facing small business, the Federal Government needs to provide a level of protection for lawfully approved company or business names against use or exploitation by another party, including a company or business. Specifically, any company or business should be entitled as of right to have its lawfully approved name as its domain name. If such protection is not provided, small business will not be able to take any effective preventative measures against:

- Trade practice violations
- Identity theft, fraud or compromise
- Privacy violations
- Adverse behaviour of another company

The basic assumption of any business is that it will continue as a going concern. The current combination of the lack of Government legislation and regulation with a domain name policy exploiting this situation, could result in a viable business having to close down. The impact of small business closures should be well known to Government.

What competitors may not have been able to achieve lawfully; the internet literati has handed to them on a plate – our business identity.

As self-regulation by auDA has not worked in this area, Government now needs to regulate to protect business names as domain name so that business can establish effective crime or adverse activity prevention strategies. Small business cannot afford the normal legal approach of wait until it happens, and then expect justice.

Moreover, domain name policy should be reviewed to ensure that it is neither perceived nor actually creating victims of preventable internet related crime.

The policies allowing the confusion of identical names belonging to different parties need to be redressed urgently to prevent even the slightest perception that internet related crimes could occur and be attributed to errors of policy, or gaps in the policies.

This submission is based on three years of experience in dealing with trying to protect the identity of my small business on the internet. It is not hypothetical; it is as real as daylight.

My specific case is as follows.

My company name is Logistics Pty Ltd, which I formed in 1987. In 1994 I applied for the domain name www.logistics.com.au. This was declined because at the time, as I was told by the ISP, that only 8 character names were being accepted. So, I settled for www.logistic.com.au. In 1999 I noticed there were longer names so I asked my ISP to vary my domain name by adding an "s" to align it to my company name. This was declined by MelbourneIT on the grounds that logistics was a generic word. The final outcome in accordance with auDA policy will more than likely result in my company name being given to another company as their domain name. So, there will be a company of some name (it may not even have the word logistics in its name) with the domain name www.logistics.com.au and my company called Logistics Pty Ltd with a domain name of www.logistic.com.au.

If you have any questions, please do not hesitate to contact me. Also, I am available to discuss this matter with members of the Committee.

Adrian Stephan (MMgt, Grad Dip Mgt, CPL)
Managing Director
Logistics Pty Ltd
90 Bruce Street
MT WAVERLEY VIC 3149

Ph: 03 9888 2366
Fx: 03 9888 2377

email: adrian.stephan@logistic.com.au