

## Domain Name Debacle

The situation exists where a legitimate company name can be given to another company as its domain name. This can introduce a wide range of consequential risks to the company whose name has been given to another party as its domain name.

Using Australian Standard/New Zealand Standard 4360 Risk Management as a risk management analysis method, the high to extreme risk levels a company faces when it is prevented from having its company name as its domain name include:

- trade practice violations;
- privacy violations;
- identity theft, fraud or compromise; or
- adverse image due to the behaviour of the other company.

The outcome for any small business is the risks of high financial or legal costs may force the closure of the company.

The problem is caused because company names are not fully protected against exploitation by other parties. Although there have been many attempts to establish the integrity of names with the introduction of programs such as the Australian Company Number (ACN), these initiatives have not been sustained regarding domain names. In fact, the situation is even more logically bizarre. To get a domain name you must have a company name or a business name with and ACN or RBN. However, that does not give the company (or business) the right to have that name as its domain name. In fact, under current practices the name could be auctioned-off or otherwise distributed to another company.

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

[http://www.accc.gov.au/ecommerce/CPGuidelines\\_final.pdf](http://www.accc.gov.au/ecommerce/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.”

Notwithstanding this guideline, the outcome of the domain name policies as implemented in my 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](http://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 on the grounds that logistics was a generic word. The final outcome looks like there is an extremely high probability that my company name could be 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.

Does this comply with the OECD Guidelines, or even the spirit of the Guidelines?

On 22 June 2000 Minister Alston issued a press statement in which he stated:

“Cybersquatting is the abusive or bad faith registration of an internet domain name that is similar to a name in which another person has intellectual property rights, or some other legitimate claim.’

‘Australia is leading the world in issues of internet governance and policy discussions. Preventing cybersquatting will increase confidence in internet infrastructure and e-commerce by protecting the established rights of businesses and individuals,’ Senator Alston said.”

The Minister’s comments are correct. The problem is, that they have not been implemented. If his statements were correctly implemented then there would be some form of fair and transparent process to ensure that a company could establish its rights to its company name as a domain name. That is not the case. Some companies are having their names auctioned by auDA, or distributed by an auDA governed process, without any early intervention opportunity for a company to independently establish its legitimate claims or established rights of business or individuals, as stated in the Minister’s press release.

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. Such Regulations have precedence.

The Government introduced a regulation to protect the exploitation of the name of Sir Donald Bradman. So, Government will regulate to protect the name of a famous sportsman, but not every business in the country. Also, the Government recently changed the Custom’s regulations to overcome a problem News Ltd had with the importation of ANZAC medallions. There are probably many others that go through unnoticed.

Many are probably familiar with the Qantas cybersquatting case in New Zealand in 1999.

<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."

Such action should not be condoned irrespective of the size of the company. Although Qantas is a well known international company, many small businesses are similarly well known entities in their market place as well. The comments of Justice Anderson could apply equally to large and small companies, particularly those small companies that have been in business for many years.

If the range of Australian domain name legislation, regulations and policies block a company from exploiting its name on the internet, does Justice Anderson's opinion apply? Everyone can form their own opinion.

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 and 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”

Although large corporations are open to specific patterns of internet fraud, the same applies to small businesses as well. In the small business case there is probably a closer analogy to individual identity theft.

There are many articles in the media on identity fraud. The common outcome is that the victim is a victim for life.

Under the current processes, a company cannot take the necessary steps to prevent crimes or other actions against its identity because existing policies deny the company control over its identity. In any business there is control over who can access the premises and who can physically represent the company. However, in the .com.au domain space a company does not have the necessary level of control over its identity and is therefore unable to protect its identity and the door is open for all of the events described above to take place unimpeded.

There is an urgent need to address the policies that prevent a company from having its company name as its domain name so that it can take a crime preventative approach rather than being destroyed.

It is clear that where the name of a company could be allocated to another company (irrespective of process) as its domain name, that this will cause a much higher level of risks of internet related fraud, such as passing off.

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 fraud could occur and be attributed to errors of policy, or gaps in the policies. It could be argued that the current process amounts to “covert cybersquatting”.

The Australian Government is signatory to the Treaty protecting trading names, so why did it deliberately not protect trading names as domain names? I am sure that every small business would like to know why the Government did not protect their names in a media that is so critical to small business. From the days of PM Keating small business has been told to get onto the “Information Superhighway”, and yet the Government won’t protect our identities.

This matter is so important that a more proactive and preventative approach to policy is required. At a time when we should be tightening controls over identities; identity loopholes are being created for exploitation by criminals and others. Otherwise, the outcome will be the creation of victims of internet related crime by Government policy.

It is time for Government to protect the livelihoods of people and not subscribe to some esoteric internet altruism.

The Government should either:

1. Immediately recognize the obvious impacts of identity related fraud that could be imposed on a company because of this policy gap; and regulate the protection of company names as domain names to implement the press release of Minister Alston.

or

2. Immediately call for a halt to any process that allocates a company name as a domain name to another company. Enable a Parliamentary Committee to publicly enquire into the need to protect company names and to ensure that the CAPA report can be fully explored.

For more information contact:

Adrian Stephan  
Managing Director  
Logistics Pty Ltd  
adrian.stephan@logistic.com.au

## Logistics.com.au Background

Logistics Pty Ltd (A.C.N. 006 734 827) was formed in April 1987 and has been continuously in business since then, and always at registered status on the ASIC register.

This is the name used to promote the company and invoice all business through it.

Late 1994 I applied for logistics.com.au and this was declined at the ISP level on the grounds that it was 9 characters long and only an 8 character name could be accepted. The reason given was the registration file at Melbourne University was limited to 8 characters. I have since met a few people who encountered the same experience.

In early 1995 I was granted logistic.com.au as my domain name.

In early 1999 I contacted my ISP (UUNet) to vary my domain name from logistic.com.au to logistics.com.au to align it to my company name.

This application was rejected by MelbourneIT on the grounds that logistics was a generic word. A long discussion has continued since early 1999 over this issue as I sought an explanation that would withstand scrutiny.

The core issues are:

MelbourneIT (Jan Webster) stated that it was a difficult policy to administer and that she had to interpret it exactly as written. So, I did not expect to find violations of the policy under her stewardship. However, this is not the case and a few examples are as follows.

[www.reliability.com.au](http://www.reliability.com.au), created 19990401 belongs to a company called Asset, Reliability and Maintenance Specialists. This is an interesting case as the company name consists of 4 words. [www.asset.com.au](http://www.asset.com.au) belongs to Asset Communications, created 19970320. Maintenance and Specialists do not exist as domain names (perhaps MelbourneIT knew what the words meant). But, asset is a heading in the Yellow Pages.

[www.greengrocer.com.au](http://www.greengrocer.com.au) created 19970603. A single word heading in the Yellow Pages.

[www.woodside.com.au](http://www.woodside.com.au) created 19980402. Has two entries in the post code book and the company was named after the Victorian township of Woodside.

[www.quality.com.au](http://www.quality.com.au) created 19971020

[www.drinkingwater.com.au](http://www.drinkingwater.com.au) created 19990831, is it or is it not a compound word. It depends upon usage and is borderline and shows discretion.

[www.mtbuller.com.au](http://www.mtbuller.com.au) created 19980828, a place.

[www.vegemite.com.au](http://www.vegemite.com.au) created 20000404, is a product. The fact that it belongs to Kraft maybe a factor! Also, if it is approved on the grounds that only Kraft can use the name can also be applied in my case to Rule 6.2 as no one can trade under a company identity logistics without violating my third part rights.

[www.astrology.com.au](http://www.astrology.com.au) created 19970929

[www.fengshui.com.au](http://www.fengshui.com.au) created 19970725

[www.dentist.com.au](http://www.dentist.com.au) created 19971110

[www.dependability.com.au](http://www.dependability.com.au) created 20001011.

[www.pipeline.com.au](http://www.pipeline.com.au) created 19980714, Pipeline Internet

[www.popstars.com.au](http://www.popstars.com.au) created 19990907, imagination Holdings Popstars

[www.sap.com.au](http://www.sap.com.au) created 20020423, SAP Australia Pty Ltd

[www.flu.com.au](http://www.flu.com.au) created 20000810, CSL FLUVAX

The relationship between some of these is very interesting. They all have a strong generic flavour (how many types of sap or flu are there?), as well as between their business names and domain names.

There is an International Standard on quality, it calls up a standard on dependability, the dependability standard calls up reliability and logistics. So, why is logistics not treated the same way? Whatever applies to logistics as a profession or service applies equally to quality, asset, reliability, and dependability. I guess you have seen the oil company advertisement espousing the "dependability" factor of their product.

For clarification, International Standard IEC 60300 Dependability Management series of standards describe the scope of dependability ([www.iec.ch](http://www.iec.ch)). This IEC calls up reliability methods and in particular has an application guide IEC 60300-3-12 Integrated Logistic Support. This Application Guide then describes all the tasks, plus many others, that people perceive as logistics. So, if one perceives that logistics is something different to dependability or reliability, it can be demonstrated by an international standard that they are all related. Actually, by the hierarchy of the standard, dependability is more generic than either reliability or logistics, if we were to accept the notion that they are generic words.

Also, I think if you stopped 100 folks in the street 99 could give you a reasonable description of reliability, quality and dependability and probably 20 could give a similar description of logistics.

The Domain Name policy on generic words was as follows:

Any generic word that is defined and used to represent products, services or professions. Typically, these are words that appear in an Australian word list (e.g. The Macquarie Dictionary) and also in a commercial category listing (e.g. The Yellow Pages Index®).

The first sentence is so encompassing it probably makes the policy unworkable because it applies to so many words. The word “typically” in the Oxford dictionary is defined as: characteristic example, representative ... That is, it is not an exclusive to a word list and the commercial category listing. Further, it describes “in a commercial category listing” and gives an example as the Yellow Pages. But, if the word appeared in any commercial listing it would have to be rejected. The Yellow Pages by this language is not exclusive. If it was, the language should have been “The Yellow Pages shall be used as the sole authority.”

Overall, this phrase is so full of logic errors that it cannot be applied with precise judgement.

Also, it is interesting to look at the Terms and Conditions in the Yellow Pages, Terms and Conditions, item 4: “Pacific Access and Telstra warrant that this directory is reasonably fit for the purpose for which directories are commonly used. “ It is only reasonably fit and MelbourneIT is putting lawfully approved company names, and the continued livelihood of their owners, at risk! Also, are directories commonly used for the purpose for which MelbourneIT is using it? I think the answer is no.

Also, given that the Yellow Pages has rules on the creation of headings, etc I don't think it can be used as a definitive authority for all professions, etc. An example is integrity. There is a lot of professional activity in this field but it is unlikely that Yellow Pages will in the foreseeable future have a heading called Integrity. Therefore, is the Yellow Pages being used outside of its warranty? I believe that it is.

I think a more appropriate list would be the Library of Congress catalogue, now that list contains just about everything in the known world. There are also specialist directories that people will list in because of the limitations of the Yellow Pages. Under the policy they cannot be excluded and would have to be used as a source.

So, if I provide a Library of Congress list that includes reliability and dependability, will MelbourneIT be forced to withdraw these names?

The bottom line is that I appreciate that it is a fine judgement call, and is really a case of: “Orders and instructions are for the guidance of wise people and the slavish following of fools”.

It is not a case of the names that have been rejected that can be used as justification, it is the fact that several names have been approved that violate the rules that set the precedence.

I think the problem is that MelbourneIT made a decision, and cannot see a way to change her mind once it was made-up. I think they simply erred to the conservative in their judgement and didn't know how to recover the situation.

I speak to many people about this and the only ones who seem to think it is right is the domain name community. Everyone else uses words such as stupid, idiotic, etc and often with modifiers. I also often get the term digital terrorists.

I asked Mr Elz why single company names were treated that way in the policy. His reply was along these lines.

- Commercial categories were never relevant – the rule was that no common words would be permitted, and logistics would certainly miss out that way.
- At the time one word company names were never considered, and I would have modified the policy to allow the case.
- Had I thought about it I would have allowed the case.

I cannot find anything equitable about the position of MelbourneIT or auDA. MelbourneIT will say that some mistakes were made in the early stage. That is understandable, but most of these were at least 6 months after taking control of the policy, and that is long enough. But, these examples spread over a couple of years and this is not consistent.

Somehow it seems ridiculous to be in this position. There is only one way to solve the problem, the Federal government needs to do the job it should have done in the first place and that is look at all of the property issues in names (intellectual and real), and put in place the necessary legislation that protects business names, trademarks, etc irrespective of medium (print, electronic, word of mouth, etc). Any other approach is a bandaid.

The policy to get a domain name requires the applicant to have an ACN or ABN, it seems only logical that an applicant should be able to have the exact word linked to those numbers. But, according to MelbourneIT and auDA it is a much fairer system that some can or some can't.

The situation becomes even more ridiculous when the identical names check on ASIC for logistic or logistics only returns my company name.

## **LACA Presentation**

I refer to the preamble to the Australian Domain Names Administration Ltd (auDA) Constitution. It is important to keep this in mind. I believe it would be instructive for the Committee to find out exactly what this means and to what extent the Commonwealth of Australia has sovereign control, and who exercises it. The preamble states:

Taking the view that the Internet Domain Name System is a public asset, and that the .au ccTLD is under the sovereign control of the Commonwealth of Australia, auDA will administer the .au ccTLD for the benefit of the Australian community.

1. The consequences of domain name policy are described by a fictitious example in the submission. The following example shows how simple it is to achieve this outcome in practice. This information was extracted from the ASIC business names and Whois domain name databases Tuesday 3 September 2002.

Assume a major spare parts retailer based on the east coast wanted to start a new business on the west coast to serve the mining industry there. They wanted to incorporate the name Western Spares Pty Ltd as the business. However, Western Spares is a NSW registered business L0077811. But a check of Whois shows that the domain name [www.westernspares.com.au](http://www.westernspares.com.au) is available. So, they incorporate the company Online Western Spares Pty Ltd. This entitles them to claim and be given the domain name [www.westernspares.com.au](http://www.westernspares.com.au). Also, they could apply for and be given the domain name [www.ows.com.au](http://www.ows.com.au). But, this is the name of an incorporated company O.W.S. Pty Ltd ACN 100 944 634. The one company has stopped forever the two existing companies having their exact company names as domain names. The consequences of these "stolen identities" should be obvious; but, you should form your own views about the equity of such a situation. This case is extremely likely as, I am sure you are aware of the ABC articles on [www.ato.com.au](http://www.ato.com.au) and [www.mabo.com.au](http://www.mabo.com.au) as well as the Channel 7 Today Tonight articles on identity theft.

It also is unclear how such a scenario, that took about 3 minutes to put together, satisfies the auDA Constitution "... for the benefit of the Australian community." How is it beneficial to the Australian community that company identifiers can be legitimately given to other parties as their identifiers and thereby exclude the original owner of the identity, the use of its identity on the internet. It is counter-intuitive.

You have to have a company name to get a domain name. But, there is no right to have the company name as the domain name. Moreover, your company name can be given to someone else as their domain name. The problem of two businesses having identical names is remote and should be handled by normal legal principles based on equity rather than an ad hoc group of literati.

2. A part of the problem is that our legal systems are not preventive, they are reactive. Although it is quite obvious that either overt or covert actions resulting from a bad faith registration can be foreseen, there is no legal remedy until it happens. That is, an irrevocable victim has to be created before an action can be taken.

3. There is an urgent need for retrospective legislation or regulations to ensure the identity of any business is protected from exploitation by a third party. Self-regulation has failed small business as the auDA domain name policy does not prevent such events, and in fact openly and proudly enables exploitation by a third party. This is not a short term problem, the crime could happen many years from now. The US experience is that it can take up to 14 months to detect an identity crime.

Such regulations or variations to regulation are common and I am sure you know that better than I do. However, I would like to draw your attention to one that is very relevant.

On 12 October 2000 the Prime Minister released a statement to protect the name of Sir Donald Bradman. The opening part of the statement is:

“I am pleased to announce that the Governor-General has made amendments to the Corporations Law Regulations to protect Sir Donald Bradman’s name from inappropriate commercial exploitation.”

I recognise that Sir Donald Bradman may have been a well know cricketer. But, should his name receive any more protection from “inappropriate commercial exploitation” than any other business? In my view this is an absolute insult to any small business (regional or city) working to build and protect its business.

4. As further evidence that this matter is of great concern to small business, I have been working this issue with the Council of Small Business Organisations (COSBOA) and with the Micro Business Network (MBN). I understand the MBN has already made a submission to the Senate Committee into Small Business and Employment. That submission also identified the need to address this problem. I suggest that the Committee seek comments from these two groups on this issue.

5. In an era when we seek portability in everything from our working software tools (e.g. standard business activities and the internet would not work without them), telephone numbers, etc; it seems totally ridiculous that we cannot have portability of our business names as of right across those services that are instrumental to our businesses. The role that the internet has in our daily business activities is as critical as the telephone system. In all reality it now has an “essential service” status. So, why then has Government abdicated this critical business function to self-regulation without so much as an Ombudsman to hear complaints? I am sure you would be very well aware of the uproar that would take place if Telstra decided to auction-off someone's phone number they had held for many years.

6. By way of another example I teach a unit in reliability engineering by off-campus learning with a major university. I have students from many parts of the world (UK, Middle East, Africa, USA, Asia, New Zealand, etc). I receive most of my enquiries and assignments from them via email. They might not be aware of the finer points of auDA policy; but, should their privacy as a student be put at risk? Would you want for yourself or for your student child to have assignment information, grades, personal information or explanations, etc using a system that could be easily compromised without either them or a teacher knowing? Besides, it is quite possible that such an activity may contravene the laws of their country. Then who is liable? Has the Government and/or auDA failed in its duty of care?

7. Similar discussion could take place on the need for security of taxation and other personal information. These are described in the submission.

8. The submission, and this presentation, has shown how this is a general problem. In the submission I also describe the specific case of my company.

As the decision in my case is without any defensible explanation by either MelbourneIT or auDA lacks any sensible logic, it would be quite reasonable for a more cynical person to form the view that some kind of conspiracy or other ulterior motive was involved to deny me my company name as my domain name.

The advice of my business associates and solicitor is that I should shut down Logistics Pty Ltd as an operating company immediately [www.logistics.com.au](http://www.logistics.com.au) is allocated to another company as I would be unable to afford the continuous threat of litigation, identity problems, etc. My fear is that this domain name registration to another party will lead with almost certainty to internet related crimes as described in the submission. This fear is well founded based on current known experiences. Thus, closing down my 15 year old small business is the only practical option to prevent internet related crimes against it. Tomorrow morning on September 10 at 9AM my legitimate company name goes up for auction as a domain name, and at 11AM Wednesday morning on September 11<sup>th</sup> I will know if I have to close my company. So, this might be the last time I make a presentation as Managing Director of Logistics Pty Ltd. In other words, death by bureaucracy.

9. In the language of criminologists on crime prevention, the Guardian must step-in quickly to prevent crimes against any business through exploitation of its name or identity by a third party. You represent the Guardian with sovereign control in the Commonwealth of Australia - Parliament. Refer back to the auDA constitution preamble.

Lord George stated early last century that the business of war was too important to be left to the military. The analogy in this century is that the importance of cyberspace is too important to be left to its literati.

I appreciate that this is a complex problem with many issues to be considered. But it needs to be solved by a rationale that is to the benefit of the Australian community. I do not think it should be solved by a cheque-book as is the current method.

The Australian Securities and Investment Commission requires, amongst many other rules, a director:

1. You have to be honest and careful at all times, and you have to know what your company is doing.
2. You must act in the company's best interests, not just your own interests.
3. Any information you get through your position must be used properly and in the best interests of the company. It is a crime to use that information to gain, directly or indirectly, an advantage for yourself or for any other person, or to harm the company. This information need not be confidential; if you use it the wrong way and dishonestly, it may still be a crime.

I am trying to be honest, careful and protect the company's best interests by trying to prevent a range of crimes against it that will happen under the current domain name policy. But, I can't do that.

Point 3 actually raises a very interesting issue. Say, your company was made aware that it could obtain the name of another company as its domain name. The problems of cybersquatting, typosquatting, bad faith registrations, etc are all well known. Would taking the name of another company as your domain name violate this rule as a director? Is it a harm to the company to put it at risk of prosecution for bad faith registration of a domain name?

I, and many other small businesses, need to have legislative or regulatory processes in place so that we can take all necessary steps to prevent crimes against the most critical element of our businesses – our names and identity.

Small businesses urgently needs to have their names protected against exploitation that could make them innocent victims of internet related crimes. I urge you to move quickly to start the prevention process before more small businesses are turned into victims. It is quite possible that in the time I have spent here so far that businesses have been disadvantaged by this anomaly and their status as victim could take months to years to be known.

There is an old proverb that states that "Good fences make good neighbours". In the context that we want good fences to define our property from another person's property, then similarly we need good legislation, regulations and policies as fences to protect our business property in all of its forms. Before the internet we knew the identity risks that we normally had to contend with. However, it is unbelievable that Government actually enabled the self-regulated internet group to introduce policies that significantly increased the risk of crime rather than reduce it.