



Issues for Consumers in Global Trading
Louise Sylvan
ACCC Deputy Chair
Attorney-General's Department
International Trade Law Conference
23 September 2004

The past decade has seen an unprecedented opening up of the Australian economy which has helped deliver consistent strong rates of growth, low unemployment, low interest rates and high value sophisticated products and services.

Spurred by innovations in communications, financial services and information-based technologies, Australian firms now compete against the rest of the world. Our markets are no longer sheltered by barriers of information and much less so by distance. With the integration of markets, world's best practice is often the necessary benchmark for efficient supply and nations increasingly strive for trade advantage through innovation.

This is great news for consumers, who now have the entire world just a click away to shop around for the best price on goods like an overseas holiday or a DVD – thereby, they drive better competition at home.

Unfortunately, of course, it also means those same consumers are also just a click away from a whole world of scam artists who are now no longer limited by geography. Courtesy of the internet they too now have a vast global market.

In many ways, the scams on the internet are not much different from those that have been around for decades – pyramid schemes, fake lottery wins, miracle health cures – I'm sure if you have an email account you've seen them all at some time.

But what the internet has allowed those behind the scams to do is to globalise their operations and in a far more efficient fashion than they ever could achieve door to door or through the mail.

Take the Nigerian letters for example. I'm sure many in this audience were at one time honoured by a very respectfully worded letter with a tale of vast sums of money needing to be transferred out of Nigeria and asking for your bank account details.

Those behind the letters knew that maybe only one in a thousand – possibly only one in ten thousand - will fall for their scam, but even that one would be enough to offset their mailing costs and make them a tidy profit. Email is only a fraction of the cost of a postage stamp and much quicker – now, those behind the fraud can afford to send millions and millions of emails out to potential victims.

Suddenly, the costs of the scam have fallen, and the potential gains have increased substantially, whether it be miracle weight loss products, financial plans, pyramid schemes or surprise wins in foreign lotteries you never even purchased a ticket in.

And it's not just consumers who are the targets. With business increasingly relying on the internet and the speed, ease and lower cost of email, many of the old scams and swindles have been updated.

These scams rely on the assumption that business operators, particularly in small business, are very busy, and will give them the information they ask for without thinking about it.

The classic example of this is fake billing, which often involves advertising or entries in trade magazines, professional journals or 'business directories', for which the perpetrator of the scam seeks payment for unsolicited goods or services.

Sometimes the ad or entry will take place, sometimes not, but either way, the business is tricked into paying for something they did not order and presumably did not want.

The internet has also allowed the scam artists to develop **new** ways of parting people from their money, often by exploiting the lack of technical knowledge most of us have about the way the internet works.

Domain Names Australia

The ACCC commenced proceedings against Domain Names Australia Pty Ltd and its director in October 2003, alleging that the company had breached the Act by sending out misleading or deceptive notices inviting the recipient to register and pay for a particular internet domain name.

In many cases the name referred to in the notice was similar to the recipient's existing internet domain name – for example, a business with the domain name 'www.mybusiness.com.au' may have been sent a renewal notice for 'www.mybusiness.com'.

The Federal Court found that the form of notice conveyed a number of false representations, including

- that the registration of the recipient's existing domain name had expired or would expire if payment was not made by the 'Return Date';
- that Domain Names Australia Pty Ltd was offering to re-register or renew the recipient's existing domain name; and
- that the recipient would be required to pay the amount mentioned in the notice to maintain the registration of his existing domain name.

The court stated that "many [persons] who receive the notice will know very little about the internet and the use and registration of domain names. These recipients will include first time users of the internet and unsophisticated Registrants of domain names".

The court went on to note that where the recipient of the notice was a large organisation with a separate accounts department "there is a greater risk that the reader [the person in the accounts department] will have little or no knowledge about the internet, the registration of domain names, or the fact that it is possible to obtain registration of very similar domain names".

The Federal Court declared that Domain Names Australia had breached section 52 of the Trade Practices Act and that its Director, Mr Rafferty, had been involved in this contravention - making orders restraining the company and Mr Rafferty for a three year period from engaging in future offending conduct of this nature.

In a unanimous judgement just this month, the full bench of the Federal Court dismissed an appeal by Domain Names Australia and ordered them to pay the ACCC's full costs.

I should point out that for a number of reasons, it was not possible in this case for the ACCC to seek restitution on behalf of the thousands of businesses tricked into paying Domain Names Australia.

As I have pointed out in other forums, a claim for compensation for the victims is problematic under the Trade Practices Act as there are restrictions on the ACCC seeking relief for non parties.

However, auDA (the policy authority and industry self-regulatory body for the .au domain space) has also instituted proceedings for breaches of the Trade Practices Act against Domain Names Australia. These proceedings, which are still on foot, are being run as a class action for compensation.

Phishing

Another classic example of the internet spawning inventive new frauds is the fraudulent bank emails.

Some of these are very simplistic – we are your bank, please send us your account and PIN number. Others are a little more sophisticated and claim that there has been an attempt to defraud the account and they want to check the numbers.

But the most sophisticated told people that the bank had changed its internet address, gave the new address with a link, and told people to log on there. These sites looked just like the original sites, but once you logged on, they captured your number and pin and within minutes your account could be cleaned out. This is an activity known as “phishing”.

As most, if not all of these types of scam originate from overseas, it makes it that much harder for Australian authorities to find the perpetrators (even if we do identify them), to get the money back or to launch a successful prosecution.

Which is of course one of the main reasons why those who perpetrate these scams base themselves overseas.

But we have had some success. And with our focus on global co-operation, we expect to have more success.

www.sydneyopera.org

Last year the Federal Court ruled an imitation Sydney Opera House website which operated out of the United States had misled and deceived customers.

In that case, a Mr Richard Chen operated the website www.sydneyopera.org, which claimed to be the official booking site for the Sydney Opera House.

The ACCC alleged that several consumers from the United Kingdom and Europe tried to buy tickets through the imitation sites. Although their credit cards were charged, they were either overcharged or did not receive the tickets.

The ACCC's case involved complicated technological issues, compounded by the fact that the operator and websites were both based in the United States.

While we were not able to obtain restitution for the victims, we were able to stop the scam by acting in conjunction with our counterpart agencies around the world through the International Consumer Protection and Enforcement Network (ICPEN).

The Federal Court ordered that the site be closed down and the United States Federal Trade Commission assisted the ACCC in bringing this order to the attention of the internet service providers which had hosted sites involved in the misleading conduct.

Worldplay

Another victory came just this month when the Federal Court found Gold Coast company Worldplay Services Pty Ltd breached the Trade Practices Act by participating in an international online pyramid selling scheme.

Its director, Mr Greg Kennedy, was also found to be knowingly concerned in the contravention. Both decisions are on appeal.

The Australian Competition and Consumer Commission alleged, and the court found, that World Games Inc, which operated internationally using a website, was an illegal pyramid scheme.

The scheme is fragmented, with a company in the British Virgin Islands having overall control, and service companies contributing to the scheme operating from Britain, Gibraltar, the Netherlands Antilles and Australia. Consumers recruited into the scheme came from a number of countries, including Canada, the United Kingdom and Norway.

The court's ruling clearly establishes that no matter how internationally fragmented a company makes a scheme, in order to avoid jurisdiction, the new pyramid selling provisions of the Act will catch the scheme, and make it liable to prosecution.

In short, Australia will not be a haven for the operation of these schemes

Again, we worked successfully here in cooperation with a number of overseas regulatory bodies, and proceedings continue in other jurisdictions regarding this scheme. The Royal Canadian Mounted Police has taken criminal proceedings against Canadian participants.

Online purchases

I should stress that the Commission is not trying to warn people off using the internet for transactions. The internet can be a safe, convenient and cheap way for consumers to purchase goods and services and a great facilitator of 'the right to choose'.

The most recent figures from the National Office of Information Economy show 10 per cent of Australians now purchase goods on-line, 23 per cent pay bills on-line, and more than a third use the internet for banking.

As consumers grow more confident in conducting transactions over the internet, it's clear much more needs to be done to ensure not only that regulators are vigilant and co-operative all over the world, but also that consumers are better informed about their rights, and what they can do to protect themselves.

One way we have sought to assist consumers is through a booklet and campaign launched earlier this year by the ACCC with good advice on what consumers can do to help protect themselves from scams when using the internet.

The booklet includes advice such as:

- avoid unsecured websites that insist on personal details or up front payments
- install software that protects their computer from viruses and unwanted programs, such as internet dialling programs that cause hefty phone bills through modem hijacking
- check that the internet address matches the site.
- do not access banking and ticketing sites from email links; and
- when it comes to spam or junk email – delete, delete, delete!

But as well as consumers being aware of their rights, businesses must also be aware of their responsibilities under the Trade Practices Act when trading online.

Unfortunately, it appears many companies are either not aware of these responsibilities, or somehow believe that the Trade Practices Act doesn't apply when it comes to the internet.

Earlier this year the ACCC led consumer protection agencies from 24 countries in scouring the internet to uncover shonky websites which are 'Too Good to be True', as part of the sixth International Internet Sweep, held in February.

Globally a record 1847 suspicious sites were flagged by sweepers. The majority of suspicious websites identified by the ACCC were work at home schemes which grossly exaggerate earnings potential, lottery scams, pyramid selling schemes, get rich quick schemes, prizes and free offers which were not actually 'free' and educational offers.

The lure of quick, easy money and opportunities to work from home entice vulnerable consumers into such schemes. Common pitfalls include start up fees, added costs, and grossly exaggerated earning potential, often resulting in thousands of dollars lost after being poured into internet scams.

While these sorts of websites clearly have only one aim in mind, to rip off anyone gullible or unlucky enough to trust the operators, just as concerning is the fact that many otherwise respectable businesses appear to believe the Trade Practices Act somehow doesn't apply on the net.

More recently, the ACCC surveyed the 1000 most visited Australian websites by Australian consumers and the findings were very concerning.

Of the 1000 sites, 334 were transactional—that is, sites offering goods or services online – and of these only 265 contained online terms and conditions (which is not in accord with the Treasury's Best Practice Guidelines).

Unfortunately, in many cases these clauses raise significant concerns.

Of the 265 transactional websites which contained a written contract:

- 54.3 per cent had a clause attempting to disclaim responsibility for the accuracy of information posted on the site
- 50.9 per cent had a clause which attempts to disclaim warranties
- 66 per cent had a clause which limits liabilities
- 43.8 per cent had **both** a disclaimer of warranties clause **and** a limitation of liability clause.

Some of these clauses, while far from best practice, were not inconsistent with consumers' rights and remedies under the Trade Practices Act—for example, they appear to limit liability only to the extent permitted by the Act.

However, other clauses did raise concerns because they misrepresent consumers' rights. They failed to convey the level of protection consumers can expect under Australian consumer protection legislation.

Others clauses went further still, attempting to exclude basic statutory rights which are implied by the Trade Practices Act and cannot be excluded.

Because of these results the ACCC launched a campaign to make both businesses and consumers aware of their rights and obligations when trading on the internet.

In short, the Trade Practices Act DOES apply to the internet, and business and consumers have the same rights and responsibilities trading on the internet as they do in a regular store.

Spam

Another example of how the internet is both a boon and a hazard is spam - unsolicited commercial email.

Such messages are a serious annoyance for home users; as well, spam email can have significant effects on business owners and operators - leading to increased costs and hampering the ability of the business to communicate with its clients, customers and suppliers.

Currently spam accounts for over 60% of all email. These include ads for get-rich-quick schemes, adult web sites and products, software and miracle cures.

As you are aware, under new Australian legislation – the Spam Act 2003 which came into effect on April 10 this year - it is illegal to send, or cause to be sent, ‘unsolicited commercial electronic messages’ that have an Australian link. A message has an ‘Australian link’ if it either originates or was commissioned in Australia, or originates overseas but has been sent to an address accessed in Australia.

The Spam Act is administered by the Australian Communications Authority and the ACCC's role relates to any relevant breaches of the TPA that may be included in or as a result of the spam such as misleading or deceptive representations.

The Australian Spam Act covers all electronic messages – not just emails, but mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (iM) – of a commercial nature. However, it does not cover voice or fax telemarketing. The legislation sets out penalties of up to \$1.1 million a day for repeat corporate offenders.

To comply with Australia’s spam laws, any electronic message sent by an Australian business must meet ALL of the following conditions:

- Consent – it must be sent with the recipient’s consent. They may give express consent, or consent may be inferred from their conduct and ‘existing business or other relationships’
- Identity – it must contain accurate information about the person or organisation that authorised the sending of the message
- Unsubscribe – it must contain a functional ‘unsubscribe’ facility to allow the recipient to opt out from receiving messages from that source in the future

Any message that doesn’t meet all three of these conditions is defined as spam.

It’s worth pointing out that a message doesn’t have to be sent in ‘bulk’ to numerous addresses to be considered spam – under Australian law, a single electronic message can also be considered spam.

It’s therefore important that businesses and government agencies that have existing databases of customers, or are in the habit of simply adding anyone who contacts them to a database, seek the permission of everyone on these databases before sending them further emails.

Australia has a strong law in this area and it will go some considerable distance in helping to protect consumers.

International Co-operation

Spam is just one of the many competition/consumer protection problems that transcend national boundaries.

As I have already pointed out, it is very difficult to enforce Australian court orders for breaches of trade practices law against an overseas resident, or to demand of people in other countries information about scams and breaches of the Act.

The ACCC therefore recognises the importance cooperating with our international counterparts to overcome some of the challenges posed by the global marketplace.

Our involvement in forums such as the International Consumer Protection Enforcement Network (ICPEN), which consists of consumer protection agencies from over 30 countries is also important to help us tackle cross border conduct.

In 2003 the OECD adopted the 'OECD Guidelines for Protecting Consumers Across Borders from Fraudulent and Deceptive Commercial Practices'. Member countries, which of course include Australia, must comply with the Guidelines by 2006, and we are examining our current arrangements to ensure compliance by that date.

At a bilateral level, the ACCC recently signed a Memorandum of Understanding with agencies in the United States and the United Kingdom and the Australian Communications Authority (ACA) to fight spam. The MOU provides a framework for us to work together to tackle cross border spam violations and will enhance the ability of each agency to enforce their respective laws against spam.

There exist a range of other bilateral and multilateral arrangements to help move us towards more effective global enforcement.

In our recent submission to the Productivity Commission on Australia and New Zealand Competition and Consumer Protection regimes ACCC pointed out a number of ways in which our laws could be enhanced to improve cross-border cooperation in consumer protection matters.

These included increasing the ability of the ACCC to share information with New Zealand at the investigation stage to overcome the obvious difficulties for both jurisdictions in trying to piece together evidence to make a coherent case when some players may be residing in each of our jurisdictions, as well as developing laws on the reciprocal enforcement of judgements so that when a judgement is obtained in New Zealand, it may be relied on by consumers in Australia.

Conclusion

So to conclude, a more open and global trading regime has important positive outcomes for Australian consumers in terms of choice and price/value offerings. Shopping online improves that, and the internet has been a great boon for Australian consumers and business. It's a good resource for consumers and for business it removed geographic barriers and allowed them to compete for markets way beyond our modest population, enabling Australia to enhance its competitiveness.

And as the figures for online purchasing, bill-paying and banking confirm, Australians are embracing this new world of global on-line trading with some vigour. The downside is that the scamsters have become smart about the technology too and honest businesses, consumers, and regulators need to do more to ensure that shopping and transacting online is just as safe as shopping in person at the mall.

Thank you.