Cyberspace: The new international legal frontier

Keynote address to the Council of Europe Convention on Cybercrime

23 November 2011

CHECK AGAINST DELIVERY

Acknowledgements

- Thorbjorn Jagland - Secretary General, Council of Europe
- Philippe Boillat - Director General of Human Rights and Law, Council of Europe
- Council of Europe delegates
- Distinguished representatives
- Ladies and Gentlemen

Introduction

It is a pleasure to be here with you today to commemorate the 10th Anniversary of the Council of Europe, Convention on Cybercrime.

It is also a great honour to represent Australia and to convey to you that with the endorsement of the Australian Parliament in the New Year, Australia will join the 32 parties of the Council of Europe, Convention Australia will be an active member of this Convention simply because the modern ever changing world demands it.

Digital Australia

Not so long ago, commerce between Europe and Australia meant a three month voyage by boat.

Distance and isolation were a security blessing but a commercial curse for the world's biggest island.

Those days are long gone.

By virtue of technology, Australia is connected with the rest of the world like never before. We are now a driving force in the fastest growing region in the world.

The Internet has literally been revolutionary in breaking down the tyranny of distance to our trading partners.

As consumers, Australia has more than 11 million internet subscribers in a population of less than 23 million. We are home to more mobile phone subscriptions than people.

Because of its vital importance, our embrace of technology will shortly go to a new level as we build Australia's national broadband network.

A network connecting 93 per cent of homes, schools and workplaces with optical fibre and 7% with next generation fixed wireless and satellite.

This is the biggest and most expensive infrastructure investment in Australia's history.

The fact we are pursuing such a monumental piece of nation building and doing it in uncertain global economic times is obvious recognition of the importance of cyberspace.

In short, having an efficient, safe and secure Internet is absolutely vital to our individual and collective interests.

And achieving this is a significant challenge because we are all too aware that there is a duality in this modernity.

Duality of modernity

There are overwhelming positives.

The connectivity that helps young people in real time share stories, ideas and ideals. The sort of connectivity that gives people confidence to stand up for their inalienable human rights and gather together to demand the end of oppressive totalitarian regimes.

There is real time connectivity allowing global leaders to have discussions and make decisions with the speed and decisiveness necessary to respond to an emergency and save lives.

Locally, connectivity that enables a medical specialist in Sydney to look over x-rays taken in Brisbane and consult a patient 1000 miles away in Australia's glorious but remote outback.

We live in an exciting time. The internet has become an integral part of our Government, economic and social interactions.

But we are all too aware that there is the other side.

The internet also offers the darker side of the human condition – the opportunity for crime and for exploitation.

Organised criminals, scammers, fraudsters, paedophiles and agents of commercial and state based espionage have all been aided by the normative inclusion of technology in our lives.

Our duty therefore is clear - to fight the threats posed by the modern criminal. And, in this area, it can only be done effectively by international cooperation.

Developing international law

In developing international law we confront the challenge that lawmakers have faced generation after generation - the challenge of ensuring the law keeps pace with progress in the name of safeguarding the rights, property and privacy of our citizens.

Consider that in the wonderful city we gather in today, more than 550 years ago, Johannes Gutenberg perfected and unveiled the secret of printing.

The printing press was a technological development that delivered unparalleled benefits. Education, creativity and wealth creation all took incredible strides forward. Literacy rates dramatically increased, the science community blossomed and democracy spread. This technological development like many before and after it, necessitated the development of new laws.

In response to the printing press, the international community was forced to legislate in whole new fields of law relating to intellectual property, defamation and controls to reflect public moral standards and to prevent exploitation. A plethora of laws have also developed in respect to the discovery and production of documents in legal proceedings.

Similarly, we should face the legal challenges of the internet like those before us dealt with the legal challenges created by the printing press.

I therefore invite those countries that are yet to take steps to become a party to this convention to now act.

As a legal tool, the Convention will actually become stronger and stronger with every additional member state.

And there are sound reasons to become a party.

The modern cybercrime scourge

According to industry, cybercrime claimed 431 million adult victims last year and cost 114 billion US dollars. More than two-thirds of online adults have been victims of cybercrime at some point in their lives.

My country, as a connected, technologically advanced society is clearly in the sights of cybercriminals. The overall risk of cyber crime to the Australian economy is more than a billion dollars a year.

Last year alone, major cyber intrusions cost Australian organisations an average of $2 million per incident and over 200 attempted cyber intrusions against our Department of Defence alone were investigated.

Criminals are increasingly organised and sophisticated and they will look to areas that have promise of high return with low risk of apprehension. The internet provides that opportunity.

The Internet is international and criminals will take refuge in perceived safe havens. Our response must therefore be a global response.

For our part, there is no doubt that once Australia has taken the necessary steps to provide for accession to the Convention we will be better placed to take on cybercrime challenge globally.

Our domestic laws will criminalise more nefarious cyber activity. And our crime fighters will have the right modern tools for cyber combat.

Information required to prosecute cyber criminals will be protected from destruction whilst law enforcement agencies seek warrants for its access.

Evidence will be sent and received from our allies because cybercriminals don't respect national borders. At the same time the Convention requires that safeguards are in place to respect privacy and due process.

However, although the benefits are clear - our accession hasn't been without controversy. It may be instructive, for countries considering accession, for me to briefly outline some of the debate.

Australia's accession

Whilst most stakeholders supported accession, some had particular questions.

These included:

1. Concerns that obligations in respect to preservation of data did not introduce a mandatory data retention scheme.
2. Concerns that legitimate activities such as the use of software that is subsequently adopted by cybercriminals does not result in criminal charges;
3. Concerns about the adequacy of measures to ensure that Internet Service Providers and other countries would protect the privacy of information preserved or disclosed under the Convention.

Australian laws regarding the power of law enforcement agencies to deal with criminal matters recognise the primacy of key values like privacy and the freedom of individuals to express thoughts and ideas in our society.

However, Australians also expect governments to take steps to protect their safety, security and property rights.

This means that privacy rights are not unfettered but, where privacy interests are affected by national security or law enforcement measures, the intrusion must be proportionate to the outcome sought. The laws must operate within a framework that clearly defines the checks, balances and limitations within which the intrusion must operate.

We believe our law reforms are consistent with those values.

Moreover, those who have argued against the introduction of laws required under the Convention have tended to overlook the fact that the nature of crime over the Internet is all too often itself an egregious abuse of privacy and other fundamental rights.

Issues of identity theft and espionage involving access to employee records revealing financial and other personal information of employees are just two examples. Predators intruding into a living room computer to seek to exploit children by way of an online chat room is another even more reprehensible example.

Moving forward

In retrospect, the foresight of the drafters of this Convention has proven to be quite remarkable. And any suggestion that it is out of date is totally without foundation. A reading of the Convention shows that it is about practical co-operation. For example; Article 24 requires parties to provide real time assistance to one another and, Article 35 requires that assistance be made available on a 24 hour 7 day a week basis facilitated through a central contact point. This is commonsense and efficient.

While technology has unquestionably developed exponentially in the decade since the Convention came into operation, its framework and practical mechanism are still relevant. Again, for example, Article 35 requires parties to ensure that their law enforcement responders are properly trained and equipped and, further, parties have an obligation to provide appropriate technical assistance to others.

Through this practical approach, the Convention remains the world's leading international legal tool to combat cybercrime. The Convention has been effective, it continues to be effective and will become more so with an increasing number of countries becoming a party to the Convention.

And that will happen. Based on signatories and invitations more than two dozen countries will soon join.

Together we can rise to the challenge and ensure that Governments, businesses and individuals realise the full benefits of cyberspace whilst ensuring current and emerging risks are managed.

In conclusion I, once again, thank the Council of Europe for inviting Australia to accede to the Cybercrime Convention and for inviting me to speak to you today.

Thank you.

ENDS