Combating cybercrime

The Internet has changed global communications and redefined the way we do business, but it has also given us a new form of illegal activity – cybercrime.

Hacking, virus propagation, web site vandalism and denial of service attacks are 21st Century crimes that are costing companies worldwide around three trillion dollars a year. To combat this growing problem, cybercrime legislation was recently introduced into the House of Representatives by Attorney-General, Daryl Williams.

"Updated laws are vital if authorities are to effectively detect, investigate and prosecute cybercrime activities," Mr Williams said. "The proposed new computer offences and investigation powers in the Cybercrime Bill are a significant development in the fight against these activities and will place Australia at the forefront of international efforts to address the issue of cybercrime."

The Cybercrime Bill 2001 seeks to create seven new computer offences that would replace existing outdated computer offences in the Crimes Act. The new offences include:

- five or more years imprisonment for accessing or modifying computer data or impairing electronic communications to or from a computer with the intention of committing a serious offence;
- up to 10 years imprisonment for unauthorised modification of data held in a computer where the person is reckless as to whether that modification will impair data; and
- up to two years imprisonment for impairing the reliability, security or operation of any data held on a Commonwealth computer disk or credit card or other device.

It will also be an offence to possess and supply data or programs that are intended for use in the commission of a computer offence. People who possess or trade in programs and technology designed to hack into or damage other people's computer systems would face up to three years imprisonment.

The legislation seeks to provide law enforcement officers with enhanced investigatory powers relating to the search and seizure of electronically stored data.

"The large amounts of data which can be stored on computer drives and disks and the complex security measures, such as encryption and passwords which can be used to protect that information, present particular problems for investigators," Mr Williams said. "The proposed enhancement of search and seizure powers will assist law enforcement officers in surmounting those problems."

According to Mr Williams, the measures contained in the Cybercrime Bill are vital to protecting the security, reliability and integrity of computer data and electronic communications and remedying the deficiencies in existing laws. "By addressing the threats posed by cybercrime activities," Mr Williams said, "the bill will strengthen community confidence in the use of new technology and provide a means of ensuring that the benefits of that technology are not compromised by crime."

Where can I get the details?

- The progress of bills can be checked from the Daily Bills List on the Internet at **www.aph.gov.au/parlinfo/billsnet/blist.pdf**
- The text of bills and the explanatory memoranda which explain them are available on the Internet at **www.aph.gov.au/parlinfo/billsnet/bills.htm**
- The debates on the legislation can be found on the Internet at **www.aph.gov.au/hansard**

Illustration: Pat Campbell