Cyber Law in Australia

Derived from the renowned multi-volume International Encyclopaedia of Laws, this practical guide to cyber law--the law affecting information and communication technology (ICT)--in **Australia** covers every aspect of the subject, including intellectual property rights in the ICT sector, relevant competition rules, drafting and negotiating ICT related contracts, electronic transactions, privacy issues, and computer crime. Lawyers who handle transnational matters will appreciate the detailed explanation of specific characteristics of practice and procedure.

Following a general introduction, the book assembles its information and guidance in seven main areas of practice: the regulatory framework of the electronic communications market; software protection, legal protection of databases or chips, and other intellectual property matters; contracts with regard to software licensing and network services, with special attention to case law in this area; rules with regard to electronic evidence, regulation of electronic signatures, electronic banking, and electronic commerce; specific laws and regulations with respect to the liability of network operators and service providers and related product liability; protection of individual persons in the context of the processing of personal data and confidentiality; and the application of substantive criminal law in the area of ICT.

Its succinct yet scholarly nature, as well as the practical quality of the information it provides, make this book a valuable time-saving tool for business and legal professionals alike. Lawyers representing parties with interests in Australia will welcome this very useful guide, and academics and researchers will appreciate its value in the study of comparative law in this relatively new and challenging field.

The council is today launching its new information campaign, Cyber Precedent, alongside the Minister Assisting the Prime Minister for Cyber Security Dan Tehan.

Law Council president Stuart Clark said a number of Australian firms have been attacked, and a key concern is the growing use of ransomware.

"That is cases where a law firm is infected or a computer is infected by a piece of ransomware, and then the lawyer or other business gets a message from the cybercriminal asking them to pay a ransom to unlock their data," he said.

"We know that the large Australian law firms are doing a lot of work to protect themselves.

"Our real concerns are for the smaller and mid-sized firms, for barristers and sole practitioners."

The breadth of sensitive data held by law firms and vulnerable to cyber attacks is significant.

"They hold information about clients, personal information," Mr Clark said.

"Commercial lawyers hold information in relation to mergers, acquisition, takeovers, all of which would be very market-sensitive.

"Commercial lawyers working on big resource projects or international transactions hold information which we know is from time to time the subject of attempts by foreign state actors to acces