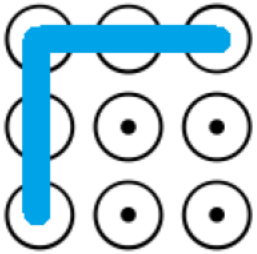
Technical Glossary

WORD	DEFINITION	NOTES
apps	An 'app' or 'application' is a standalone software program that performs a specific function or allows a user to interact with a specific online service.	Examples of apps include 'Calculator', 'Maps', 'Facebook Messenger' and 'Google Mail'.
backdoor	hidden systemic weakness in a computing system that allows the normal security barriers in the system to be bypassed	Examples of backdoors include microchips being installed onto every instance of a motherboard in a class of technology to conduct nefarious activity or provide an ability to exploit the technology at a later point in time.
cloud computing	'Cloud computing' is a general term for the delivery of hosted storage and services over the internet.	
credentials	information used by a computing system to authenticate users (for example, name, password, token, biometrics)	
data on/in apps	Apps typically need to store information such as lists of contacts, messages or user configuration settings. This data can be stored in any number of file formats or locations, including on the device itself or in 'the cloud'.	
database	A database is a computer file that stores data in a structured way, usually in a series of tables with 'rows' and 'columns'.	
database schema	A definition for how a database is structured. This may include names of tables (for example, 'Contacts') and the number and types of columns.	A simple 'Contacts' table might constitute three columns: 'Name' is a string of letters, 'Phone Number' is a series of digits, and 'Last Contacted' is a date and time.
encryption	the process of encoding information so that it can only be understood by the authorised recipient	

'going dark'	The rise of ubiquitous encryption (stored data and communications being encrypted by default), and the ease with which it is implemented within modern communications applications, has significantly reduced the efficacy of lawful interception and coverage of target data and is often referred to as 'going dark'.	
hacking	interacting or using a computing system in a manner for which it was not designed, often in order to exploit deficiencies to reveal sensitive information or obtain unauthorised access	
malware	abbreviation of 'malicious software'—a program or application that is operational on a computing system and that performs malicious activity	
pin defeat	A 'PIN defeat' is a software program which bypasses a 'PIN Lock' set by the user of a device.	The software program does not attempt to guess the 'PIN Lock'; it simply bypasses it.
pin lock	A 'PIN Lock' is a number, phrase or pattern set by the user to protect access to their device. Even if the user enables biometrics, such as a fingerprint or facial recognition, a 'PIN Lock' will still be required.	For example, '1234' or: 
rack space	physical location within a data centre where computer systems reside	A data centre is a purpose-built facility that provides stable conditions to control heat and humidity.
ransomware	a type of malware that prevents legitimate access to information	

	or computing resources until a ransom is paid to the attacker	
screen capture software	an application or built-in functionality on an electronic device that captures and stores an image of the information being displayed on the screen	
server	a computer system that serves a dedicated function or purpose, typically to 'client' machines—for example, a website	Clients interact with services provided by servers. Examples include laptops, smart phones and desktop computers.
source code	a human-readable text listing of commands or instruction to be executed by a computer	Software developers write source code to create software. The source code is compiled or translated into a machine-readable form to allow it to be executed. It typically embodies significant intellectual property and is commercially sensitive. Companies that sell software typically distribute compiled programs (machine readable) and keep their source code (human readable) secret.
spyware	software that covertly monitors activity and content on a user's computer or device	Examples include 'key loggers', which capture and forward on keystrokes; 'adware', which target users' interests; and software that captures data covertly from the inbuilt microphones or cameras on a device.
ubiquitous encryption	a term used to refer to the widespread adoption of encryption within computer and communications systems by default	Users often no longer need to proactively enable encryption or understand it. It is built into the systems they use as a default.

Legal Glossary

WORD	DEFINITION
computer	all or any part of a computer/s, computer system/s or computer network/s
designated communications provider	The term intends to cover the breadth of communications providers across the communications network, including carriage service providers, 'telcos', those who supply or install such services, and those who develop software used in connection with such services.
eligible activity	Listed activities for each type of designated communications provider—a request or notice to do an act or thing must relate to an eligible activity.
interception agency	Interception agencies are listed in the Bill and include ASIO, the AFP and various state law enforcement agencies and anti-corruption commissions.
listed act or thing	Listed acts or things are those acts or things that communications providers can be asked, or compelled, to do under the Bill.
material	material of any form, including text, data, speech, music and visual image
technical assistance notice	a notice from the Director-General of Security requiring a communications provider to do things, for the purpose of helping agencies such as ASIO perform their functions
technical assistance request	a voluntary request to a communications provider to do things, for the purpose of helping agencies such as ASIO perform their functions
technical capability notice	a notice from the Attorney-General requiring a communications provider to do acts or things directed towards ensuring the provider is capable of assisting agencies such as ASIO