The Ways Information Can Be Collected On The Internet

The first instances of concerns relating to privacy through the development of technology in Australia was recorded in 1983. The main concerns for this recommendation from the ALRC were regarding the developments in information and surveillance technology, and lead to (ALRC22) concerning legislation containing privacy principles to be introduced. Specific privacy concerns related to developments in technology included: increased storage of personal information, speed at which information could be retrieved, reduction in the cost of handling personal information, enhanced linkages between information systems, aggregation of personal information obtained from different sources, security of information systems, and increased transborder data flows. Concerns for privacy in technology was again bought up in 1988 during the reading of the Privacy Bill where the Hon Lionel Bowen MP, stated that rapid developments in technology for the processing of information had 'focused attention on the need for the regulation of the collection and use of personal information by government agencies and for an independent community spokesperson for privacy'. Again in 2000 concerns for the security of personal information discloses during online transaction provided incentive for the introduction of the private sector provisions of the Privacy Act 1988. Two recent reviews concerning privacy and emerging technologies occurred in 2005 and were the Privacy act (OPC review), and the Privacy act (senate Committee privacy inquiry). Both of these reviews recommended that there should be that there should be a wider review of these laws in Australia and that they should consider whether the Privacy act was still effective despite the developments in technology.

An area that has experienced significant reform due to technological advancements is identity management. With online transactions become a social norm many agencies and organisations now require individuals to authenticate themselves before making the transaction. Identity management systems allow trust to be built between the consumers, agencies and organisations making online transactions. In Europe they have a system called PRIME (Privacy Identity Management for Europe) and it emphasises the privacy-enhancing nature of its identity management project, allowing individuals to minimise the disclosure of their personal information online, and provides them with technical tools to negotiate privacy preferences with online entities. Another new system is the federated identity system. A federated identity system uses a central identity provider to authenticate an individual, who can then access certain other platforms without needing to re-authenticate their identity. By using an Identity Federation System, individuals can manage their identities by setting user names in various platforms and can decide what information can be displayed in different situations.

Another area that has emerged due to technological advancements is the internet. The internet is a worldwide collection of interconnected computer networks based on a set of standard communication protocols, and is a global collection of publically accessible electronic information. The internet was created in the mid 1980s and widespread use of it commenced in the 1990s, it is now estimated that 86% of households in Australia now have access to it. The internet is used for an extensive variety of social, economic and political transactions, and individuals use it to send and receive emails, e-commerce purposes, social media and government purposes. This multitude of uses and mass collection of personal information has made the internet a very common place for privacy breaches.

Currently, vast amounts of data about internet users is collected without their knowledge or consent. Examples of this include the search terms an internet user has entered into a search engine, the websites visited and the goods and services purchased or enquired about online. Just based on this data an individuals health record, education, credit history, sexual orientation and political beliefs can potentially be determined.

Another way an individuals information can be found online is via the use of cookies. A 'cookie' is a piece of information that is sent from a computer or website to an internet user's browser. The browser will then store the information on the users computer, if the user is to access the same website at a later date, the cookie will be sent back and indicate that the same user has returned to the website. Cookies are used to personalise search engines by providing targeted marketing, and also providing identification details such as a name and address to a website.

A web bug is another way that an individuals information can be collected. A web bug is a small, invisible image that is included on a web page or email, and when accessed the bug collects certain information including the IP address, the time the site was accessed, and the type of browser used to access it. Web bugs are often used by third parties, such as advertisers, to track the web pages visited by users. It has been recognised that virus scanners have varying success in locating web bugs on web sites. Web bugs are often used by both marketers and spammers to verify the validity of email addresses, as when an email containing a web bug is opened, the sender of the email is informed of the time and IP address, thereby marking the account as active.

The final way that information can be collected of the internet is through spyware and remote access software. Software or remote spyware installed on a computer can enable a third party to view the activity or data on that specific computer. Remote access can be used for beneficial purposes, such as remotely fixing a computer. However it can also be installed without the consent or knowledge of the user for malicious purposes, such as collecting personal information about the user for the purpose of engaging in fraudulent activities. Spyware can be installed on a computer in a number of ways. Whether it be physically installed through hardware, installed in the online environment attached via an email or downloaded material. In 2005, the Australian Government Department of Communications, Information Technology and the Arts (DCITA) announced the findings of their review of spyware, and concluded that the most serious and malicious uses of spyware were adequately addressed by existing laws, such as computer offences in the Criminal Code.