THE LAW SOCIETY
OF SOUTH AUSTRALIA
THE VOICE OF THE SOUTH AUSTRALIAN LEGAL PROFESSION

risk watch

JUNE 2017

Don't trust your husband with your home computer!

Further to the Technology theme of the April 2017 Bulletin, the importance of client information and computer file security is underlined by a recent story from the UK where a lawyer was fined for a failure to keep client's sensitive personal information secure.

The Information Commissioners' Office ("**ICO**"), a UK body roughly equivalent to the Privacy Commissioner, levied a fine (£1,000) on a senior barrister for the manner in which she dealt with her client's personal information on her home computer. The barrister (who practised in areas of Family Law and Child Protection) had 725 unencrypted documents, some of which contained confidential and highly sensitive information relating to up to 250 people engaged in Family Court and Court of Protection litigation on her home computer. The barrister's husband embarked on the process of updating the software on the computer and temporarily uploaded the 725 documents to an internet directory as a back up during the software upgrade. This meant that the files became "*visible*" to internet search engines and access to some of the documents could have been gained via a simple internet search.

Whilst there was no evidence that any actual damage occurred, the head of enforcement at the ICO, Steve Eckersley was quoted as saying:

> "*People put their trust in lawyers to look after their data- that trust is hard won and easily lost.*
>
> *This barrister, for no good reason, overlooked her responsibility to protect her clients' confidential and highly sensitive information. It is [not] hard to imagine the distress this could have caused to the people involved – even if the worst never happened, this barrister exposed her clients to unnecessary worry and upset."*

The legislation on with respect to privacy generally in the UK is obviously different from Australia and it may be that if this scenario occurred in Australia no fine would be imposed by the relevant enforcement bodies. It could easily be the case, however, for a similar scenario in Australia to result in a claim for damages or a charge of professional misconduct against the practitioner, especially if any confidential or privileged information did actually come into the possession of an opponent.

This story shows again how important it is for all legal practices, no matter how big or small, to take seriously the manner in which they deal with the technology used in their practices.

Large firms, for example, may have their own internal IT staff, who are specifically responsible for IT security. Medium size firms might engage IT consultants to look after their IT requirements. It is also critically important for small practices (including, obviously, barristers in light of this story) to be on top of the way they use computing technology so that it is both efficient and secure. If that involves using IT consultants then that will be money well spent. Even where a firm has IT staff, or consultants are engaged, the partners of the firm are ultimately responsible and should satisfy themselves as to the adequacy of the relevant systems.

The Law Council of Australia has compiled some excellent resources on cyber-security and cyber-risk as applicable to legal practice. Law Claims **strongly recommends** that each and every practitioner, whatever the size of their practice, spends some time looking at the extremely useful information (which includes practical tips and checklists etc) provided by the Law Council at **http://lca.lawcouncil.asn.au/lawcouncil/cyber-precedent-home**.

Don't destroy BFA files!

The topic of Binding Financial Agreements ("**BFA**") (some of which are colloquially known as "*pre-nups*") is often referred to in Riskwatch articles, and continues to be a source of regular claims against practitioners. As has been previously noted, claims in this area can arise many years after the Agreement was prepared: it is (along with estate type claims), an area of "*long-tail liability*" because the break-down of a relationship and the subsequent examination of the BFA might only occur after a long delay.

For this reason it is recommended that practitioners should treat BFA files in a similar manner as Will files.

The Law Society's **Guidelines on the Storage, Closing and Destruction of Files** recommend that Will and Estate Planning files not be destroyed until

- 50 years after the execution of the Will;
- 7 years after the confirmed death of the testator; or
- 7 years after the presumed death of the testator at 100 years of age.

The same Guidelines state that "*Consideration should be given as to whether financial agreements"* under the Family Law Act "*should ever be destroyed".* Law Claims encourages firms to not destroy BFA files so as to avoid the situation (which has happened) where, many years after the file has been closed a relationship breaks down and a claim is made against the solicitor in respect of the BFA only for the solicitor to be unable to properly defend the claim because the file has been destroyed.

GRANT FEARY
Deputy Director (Law Claims)