Forged email: lessons learned from the OzCar scandal

By Dr Bradley Schatz, Director, Schatz Forensic

By now, all but the most naïve of us are immune to the promises of Nigerian riches and the disquieting urges to action from banks which find their way into our email inboxes. Fraudulent emails barely rate any action or consideration beyond that needed to delete them from our inbox. Why then was the leader of the Australian opposition, and one of Australia's most senior lawyers besides, tripped up by a forged email?

Background

Australian media reporting was dominated during the final week of June by the OzCar scandal. Allegations of the existence of a "smoking gun" email proving the Prime Minister's preferential treatment of neighbour and friend, car dealer John Grant, led to the leader of the Opposition calling for the PM's resignation. The PM called in the AFP to investigate evidence of the email. They found a deleted copy of the email in question on the home computer of Treasury official, Godwin Grech. Preliminary investigations indicated that the email was forged. Further reports have indicated that the email originated within Treasury.

The Opposition leader, Mr. Turnbull, spent the rest of the final week of parliament defending his reliance on the forged email.

On determining email authenticity

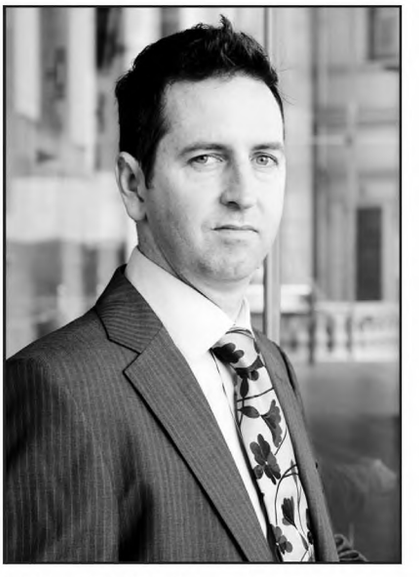
This matter highlights the need for a greater degree of scepticism when it comes to reliance on email evidence, as compared with its paper counterpart. Comparing the essential properties of the two mediums, we observe the following:

- Modification of text on paper leaves a trace, whereas the substance of email (digitally stored information) is modifiable without an obvious trace;
- Hand written signatures are distinctive and serve to authenticate the author of mail. The email equivalent of a signature is technically possible, however its use remains a niche practice and not widely observed.

Determining the authenticity of an email requires both corroborating evidence and technical expertise. Corroborating evidence can be in the form of transmission records stored hidden within the email ("metadata"), or in historical records maintained by email handling systems ("mail server logs"). Furthermore, records of the original email typically remain on the computer on which it was composed.

Email metadata is information which is stored as a part of each email but typically hidden from view. An examination of this metadata can indicate, among other things, the path that the email has taken from the sender to the recipient, and the time of receipt of the email. Careful analysis and interpretation of this information can be employed to detect tampering or outright forgery.

Mail server logs are records made by each carrier that handles delivery of an email



Dr Bradley Schatz, Director, Schatz Forensic

("mail server"). Each mail server makes a note of the receipt and subsequent handoff of the email to the next carrier along the way. These records may be analysed to prove that an email was actually sent or received. For example, in *Rana v University of Adelaide (No 2)* [2008] FCA 494, mail server logs were used as evidence to disprove the authenticity of an email. In *Montague v Montague* [2002] NSWSC 328, Austin J found that in absence of mail server logs proving transmission of a questioned email, the email could not be treated as authentic given consistent oral evidence to the contrary.

Gaining access to the computer (or iPhone, Blackberry, etc) on which a disputed email was composed may be of assistance. For example, in *NAK Australia Pty Ltd v Starkey Consulting Pty Ltd* [2008] NSWSC 1142, NAK produced a copy of the

alleged sender's work computer towards authenticating a crucial email sent from that computer. At the simplest level, identifying an email in the "Sent Items" folder of a computer will go a considerable way towards establishing that the person in possession of the computer was the author.

In absence of the former avenues for corroborating evidence, there remain further options. Emails which were hitherto considered deleted and lost may well still exist, stored in other locations. Copies of an email may additionally be stored in the senders "Sent Items" folder, in "CC" recipients mailboxes, and significantly, in archival, or disaster recovery backups maintained by the IT operators of the email services involved.

Gaining access to these evidence sources is time consuming and often involves the cooperation of multiple parties. Determining authenticity based on such evidence furthermore requires a high degree of expertise.

Commentary

It is unlikely that either Mr. Grech or Mr. Turnbull would have had access to the corroborating evidence or possess the expertise required to judge the authenticity of the email. Nor for that matter would the average email user.

Day to day, email authenticity isn't generally a problem. Our society largely manages to muddle along with email as one of our primary communications mediums. The reason it works is that each of us make decisions of trust around every email we receive.

Assuming neither Mr. Grech nor Mr. Turnbull fabricated the email, whoever inside Treasury created and sent the email to Mr. Grech relied on exploiting his trust of emails appearing to come from that source. Mr. Turnbull trusted Mr. Grech in turn.

This affair may mark the end of this kind of trust in emails as concrete evidence and the general acceptance of their authenticity. Certainly you would think so in the case of politicians attempting to score points against their opponents.

More generally, the wider implications of the increased awareness of the vulnerability of email to forgery will be felt in our courts, where emails are often produced as evidence in both criminal and civil matters.

Legal practitioners should be aware that metadata in general is discoverable[1] and consequently be prepared to produce relevant emails with metadata intact. The prudent legal practitioner will act to preserve email (including metadata) and mail server logs should authenticity later become an issue.

As for the fake email which has brought this to the public's attention, presumably the AFP is still investigating who the original concocter of the email was. This investigation should lead to an examination of the computer systems of Treasury, where traces of the email and hence clues to the original concoctor of the email may well remain. In which case, we wait with bated breath to see the next twist in this political drama.

Footnote

1. "It is clear that embedded electronic information in relation to relevant documents, including the information embodied in electronic metadata, is discoverable"[1] (Tamberlin J) *Jarra Creek Packing Shed v Amcor* (2006) FCA 1802.

Dr. Bradley Schatz is the director of computer forensics consultancy Schatz Forensic and an adjunct Associate Professor at the Queensland University of Technology (QUT). Dr. Schatz divides his time between providing forensic services primarily to the legal sector and researching and educating in the area of computer forensics. Dr Schatz is the only Australian practitioner to hold a Ph.D. in computer forensics, and one of a handful globally.

LETTERS TO THE EDITOR

A 'Letters to the Editor' section was the most popular request resulting from the 2008 *Balance* readers survey. This is your forum to make short points to the *Balance* readership; so do remember to utilise it.

Letters to the editor should be sent to Suzie Simmons at publicrelationa@lawsocnt.asn.au.