Evidence from a digital device

Council of Australasian Tribunals NSW - NSW Annual Conference

26 August 2016

Miiko Kumar

Jack Shand Chambers

Aims of presentation

- Define electronic evidence from a digital device and issues that arise from this type of evidence.
- Identify the principles relating to the admissibility of electronic evidence.
- Examine some examples of electronic evidence in litigation.

What is electronic evidence?

Wikipedia:

“Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel’s electronic door locks, and digital video or audio files.”

What is electronic evidence?

- Electronic evidence:
  1. The content (the binary data);
  2. Storage device upon which data is stored as a binary code;
  3. Software to read and interpret the binary data.

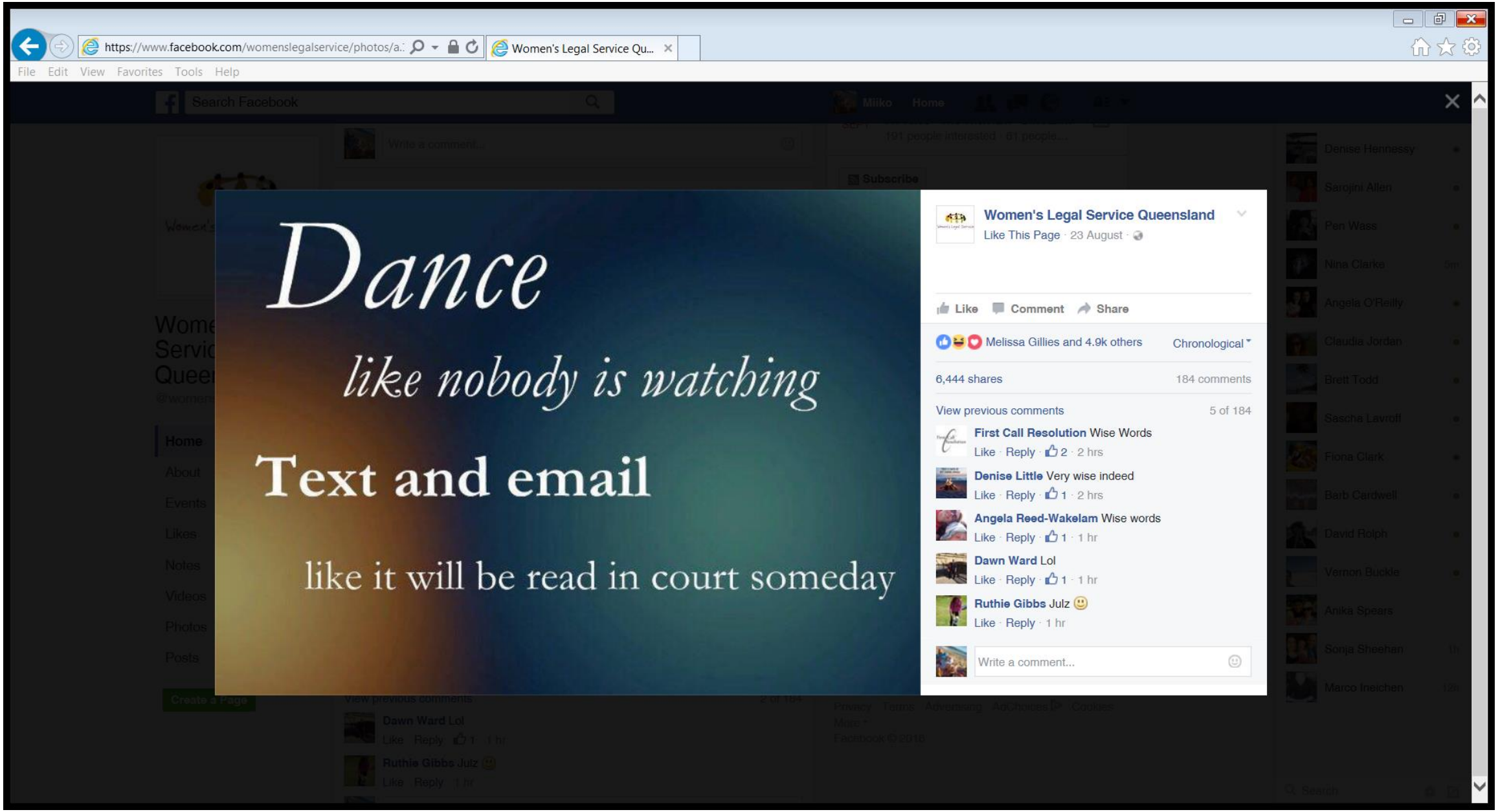
- Metadata: electronic information about other electronic data that is created by and embedded in electronic documents.

Types of electronic evidence

- Websites (webpage snapshot)
- Facebook (Facebook post, Facebook snapshot)
- SMS (print out)
- Emails (print out)
- Photographs
- Recordings (audio or visual or both)

Issues with electronic evidence

- Changing technologies
- Increasing amount of data
- Storage
- Easily created and disseminated
- Easily corrupted or changed
- Reliability and accuracy?
- Authentication: Is the electronic evidence the same as it was when it was created? (see Allison Stanfield, *The Authentication of Electronic Evidence,* (PhD Thesis, QUT, 2016 http://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf)


https://www.facebook.com/womenslegalservice/photos/a.
Women's Legal Service Qu...
File Edit View Favorites Tools Help
Search Facebook
Dance
like nobody is watching
Text and email
like it will be read in court someday
Women's Legal Service Queensland
Like This Page · 23 August ·
Like Comment Share
Melissa Gillies and 4.9k others
Chronological
6,444 shares
184 comments
View previous comments
5 of 184
First Call Resolution Wise Words
Like · Reply · 2 · 2 hrs
Denise Little Very wise indeed
Like · Reply · 1 · 2 hrs
Angela Reed-Wakelam Wise words
Like · Reply · 1 · 1 hr
Dawn Ward Lol
Like · Reply · 1 · 1 hr
Ruthie Gibbs Julz
Like · Reply · 1 hr
Write a comment...

Principles relating to the admissibility of electronic evidence

- Adduce as a document (for example, “document” is broadly defined in the Dictionary to Evidence Act)
- Relevant to a fact in issue in the proceedings
- Authenticity – possible to draw inferences as to authenticity (*Australian Competition and Consumer Commission v Air New Zealand Ltd and Anor (No 1)* (2012) 207 FCR 448)
- Presumptions to facilitate proof (for example, Evidence Act ss 146, 147 and 161)
- Hearsay (admission, first hand hearsay, business record exceptions)
- Credibility (for example, prior consistent or inconsistent statement)
- Discretionary exclusion (unfair prejudice, illegally or improperly obtained evidence)

Computer forensics

- An expert can show if metadata was changed (therefore showing that the evidence has been changed).
- Document recovery

Facebook – social networking site

- Access depends on the privacy settings.
- Example: Using a Facebook post to challenge a witness that they were not able to work in circumstances where they posted about their own business (*Kissun v Coles* [2013] NSWDC 134).
- Example: Facebook identification by victim of assault (*Strauss v Police* [2013] SASC 3).
- Example: Posting message on Facebook to serve Flo Rida (US rapper)(*Flo Rida v Mothership Music Pty Ltd* [2013] NSWCA 268).
- Example: Posting defamatory post to own Facebook page (*Rothe v Scott (No. 4)* [2016] NSWDC 160).
- Example: Posting sexual images on Facebook (*Wilson v Ferguson* [2015] 15).

Twitter

- Most tweets are publicly available
- Example: Twitter publication re defamation (*Feldman v Spinak* [*2016*] NSWSC 1083).

SMS and mobile phones

- Example: Ashby v Slipper
- Example: A mobile phone was treated as a document (*Palavi v Queensland Newspapers* [2012] NSWCA 182).

Emails

- Missing or forged emails – experts access the metadata to prove that it has been forged

Webpage

- Webpages change.
- What happens if you require a historical version of the webpage?
- Wayback Machine: *E & J Gallo Winery v Lion Nathan Australia Pty Ltd* [2008] FCA 934.

Recordings

- Can a covert recording be used in proceedings?
- *Surveillance Devices Act 2007* (NSW)
- *DW v R* [2014] NSWCCA 28
  - Private conversation, but necessay for the “lawful interest” or admissible under discretion to admit illegal evidence (s 138).
- *Prosha Pty Ltd v AXL Trading Pty Ltd (RLD)* [2011] NSWADTAP 36
- *Telecommunication (Interception and Access) Act 1979* (Cth)
- *Addenbrooke Pty Ltd v Duncan (No 5)* [2014] FCA 625
  - No proof that lawfully intercepted calls therefore prohibition on admissibility due to s 77.