Registrar experiences with WHOIS

Bruce Tonkin
Melbourne IT Ltd
WHOIS Purpose

• “Collected data should be relevant to a specific purpose, and be accurate, complete and up-to-date” - OECD Privacy Guideline

• “Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.”
  – Registration Agreement
Registrar use of WHOIS

• Registrars require access to the contact information to seek authorisations for transfer
• Registrars must also transfer the contact information to their own databases for the provision of WHOIS once a transfer is approved.
Abuse of WHOIS by third parties

• Unsolicited renewal notices (complete with expiry date and other registry data) – often aimed to mislead the consumer to believing they are dealing with their original supplier

• Unsolicited marketing of related services – web hosting, website development, email services, SPAM filters, additional domain names
  – “We saw in the WHOIS registry that you registered xxxxx.com. The next step is ….”
Abuse of WHOIS by third parties

• Fraud to collect credit card information
  – Email registrar customers, and create a dummy website with same branding as registrar
WHOIS usage

- Large registrars have around 10 bulk access agreements
- Sample stats for port 43 public WHOIS
  - 2 million queries a day
  - 137,000 separate locations
- $30 buys 30 million WHOIS records