Spyware: policy issues faced by government

Andrew Maurer
Department of Communications, Information Technology and the Arts
Australia

Spyware – technology

A variety of software:
- Keyloggers
- Data harvesters
- Remote Administration tools
- Navigation Hijackers
- Distributed processing applications
- Trojans/zombies
- Content modifiers
Or what the technology is used for?

- Identity theft
- Fraud
- Invasion of privacy
- Industrial espionage
- Other covert information gathering
- The same technology is used for other purposes – beneficial, legitimate and quasi-legitimate

Who is using the technology?

- Criminal gangs - Fraud
- Business competitors – industrial espionage
- Possibly Law Enforcement Agencies & certain Govt agencies
- Individuals
- And, at the top of the list…
The number one user…

- Companies engaged in online trade and advertising

Australia’s activities

- Review of existing legislation
- Discussion paper and public consultation
- Planning next steps
Triage

- Some things must be stopped:
  - Data theft, particularly when used for fraud
  - Invasion of privacy

- Some things must be preserved:
  - People’s right to use their computers, and the internet, safely and securely
  - The economic viability of the online environment

- Some things must be channelled:
  - Companies’ deployment of adware and cookies

Developing a common understanding

- Spyware – Any software that takes information from a computing device without the knowledge and consent of the user, and gives that information to a third party

- Malware – A diverse variety of malicious or damaging software that utilises a computing device’s processing capacity or bandwidth: viruses, trojans, rootkits etc

- Adware – Software that delivers advertising or other content that encourages the user to purchase goods or services
Developing a common understanding

- Clear, consistent definitions are needed:
  - Spyware
  - Malware
  - Adware

- A distinction between the technology and what it is used to accomplish
  - Behaviours – policy & law
  - Technology – education & tech countermeasures

Strategies

- Information and Education
- Industry partnerships
- Technology
- Legal responses
- International activity
Informing without causing panic

- Building on communication about previous e-security threats
- Stratagems for removing and preventing spyware
  www.nospyware.net.au
- For legitimate software:
  - Developing consumer knowledge and capability
  - Informed consent

Effective cooperation with Industry

- Protecting communications between businesses and their customers
- Assisting law enforcement
- Establishing standards for the appropriate use of technology
- Aiding the informed consent of customers
Appropriate technological responses

- A broad spectrum threat needs a broad based strategy
- Techniques useful against other e-security threats will aid against spyware
- A proactive, rather than a reactive stance

Targeted legal responses

- Behaviours and outcomes rather than technology
- Old crimes in a new environment – case law and precedent is needed
- Information and intelligence are critical in building successful prosecutions
International action

- A shared understanding of spyware, adware & malware?
- Following the money trail – law enforcement cooperation
- Exchange of knowledge and expertise

Thank you

Questions?

More information:
www.dcita.gov.au/spyware
Email:
spyware@dcita.gov.au