London Action Plan

Shaundra Watson
Council of Europe Octopus Interface Conference
Cooperation Against Cybercrime
Strasbourg, France
24 March 2010

OVERVIEW

- The London Action Plan (LAP) is a global public-private enforcement network organized to fight spam, spyware, and related economic and privacy threats on the Internet.

- LAP was formed in 2004 and is comprised of a broad range of public authorities, including data protection agencies, telecommunications agencies, consumer protection agencies, and appropriate private sector representatives from over 20 countries.

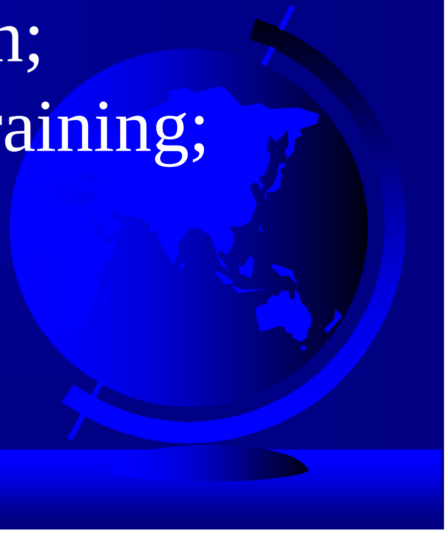
- LAP Secretariat is operated by Industry Canada, the UK Office of Fair Trading, and the U.S. Federal Trade Commission.

London Action Plan

OVERVIEW

❖LAP’s activities are focused on five key areas necessary to prevent the abuse of electronic messaging and reduce related online threats:

(1) strengthening relationships among public authorities;
(2) improving public-private cooperation;
(3) enhancing investigators’ skills and training;
(4) developing best practices; and
(5) identifying emerging threats.



COOPERATION AMONG PUBLIC AUTHORITIES

- (1) Improve public authorities’ ability to share information with or otherwise provide investigative assistance to other administrative, civil, and criminal authorities.

- (2) Identify potential partners, invite new members to join the network, and develop working relationships in jurisdictions all around the world.

- (3) Enhance understanding of how different types of authorities (e.g., civil, criminal, administrative) can use their different investigative and legal tools to work together in enforcement actions.

PUBLIC-PRIVATE COOPERATION

- (1) Improve ability to obtain and share information with private sector in enforcement matters.
- (2) Promote mutual understanding of industry and public authorities’ needs to facilitate increased cooperation.
- (3) Encourage industry recognition of various types of authorities as equal partners in the fight against spam, spyware, and related Internet threats.

TRAINING

- Enhance investigators’ skills to improve public authorities’ ability to investigate spam and spyware cases and enforce relevant laws.

BEST PRACTICES

- Formulate, share, and evaluate national and international best practices.
- Evaluate spam and spyware legislation and consider improvements.

EMERGING THREATS

- Identify emerging legal and technical threats and prepare authorities and private sector representatives to develop adequate responses.

CURRENT PROJECTS

- ❖ Membership outreach
- ❖ LEA/ISP contact database
- ❖ Training (2CENTRE and other training projects)
- ❖ Best practices survey and assessment; Cooperation with OECD on review of implementation 0f 2006 cross-border spam enforcement recommendation.
- ❖ Assessment of emerging threats at 2010 annual conference in Melbourne, Australia.

PARTNERSHIPS

- LAP has identified potential partners in the Internet and enforcement communities and intends to develop working relationships that further the objectives of the network. Potential partners include:

  - Council of Europe
  - MAAWG
  - OECD
  - ICPEN
  - Regional Internet Registries
  - Anti-Phishing Working Group
  - Other organizations or agencies in regions that are currently not well represented in LAP.

EXPLORE OPPORTUNITIES TO COOPERATE

- Overlapping issues-many spam, spyware, and related activities are both civil and criminal offenses
- Joint trainings for civil and criminal authorities
- Joint contact networks for civil and criminal authorities
- Encourage industry (ISPs, domain name registrars) to provide abuse points of contact and increase cooperation with law enforcement agencies.
- Develop collaborative model for enforcement actions that leverages resources of all relevant stakeholders