Canadian*- US Law Enforcement Internet Governance Cooperative Efforts April 19, 2010

Marc Moreau
Royal Canadian Mounted Police
Robert Flaim
Federal Bureau of Investigation

*Hockey Gold Medalists

LE Involvement

- Participation in global RIR government working groups in ARIN, AfriNIC, RIPE NCC
- Canada, US, UK, Australia and New Zealand joint cyber crime working group
  - Dedicated to joint cases, initiatives
- Participation at ICANN and introduction of LE Due Diligence recommendations
  - Drafted by Canada, US, UK, NZ and Australia
  - Supported by G-8, Interpol, Council of Europe
- Private industry initiatives, i.e., Microsoft botnet etc

RIR Government Working Groups

- Develop effective public-private partnerships
- Maintain policy and technological proficiency
- Increase international cooperation and standardization
  - Like RIRs, mimic each other
- Advocate for and against policies that effect LE, i.e., Customer Confidentiality
  - Negative impact
  - Voted down 3x
  - Residential privacy

Goal of Canadian and American Law Enforcement

We are not BIG BROTHER...

...our only goal is to work with ARIN and the other Regional Internet Registries to prevent crime and to be able to trace criminals and malefactors in the most judicious and expedient manner.

LE Issues

- IP WHOIS
  - ✓ Triage tool in tracing “owner” of IP address
  - ✓ Provides initial clues for investigation
- DNS WHOIS
- Due Diligence – prevention of criminal enterprises from fraudulently obtaining IP address space, ASN, domain names
- Knowledge and proficiency with emerging technologies

Use of Technology

- In addition to sophisticated court-ordered methods, LE uses many publicly available technologies to identify criminals, such as:
  - Domain & IP WHOIS queries
  - DNS
  - VOIP
  - Email, Instant Messenger, & IRC
  - Encryption
  - Google
  - And many others

WHOIS

- IP and domain name WHOIS information is an integral tool for all cyber investigations
- These tools provide gap analysis, target profiling, and sometimes even - identification
- **Speed and accuracy in getting the data is key**
- Even with legal process, a properly maintained WHOIS is necessary

WHOIS - Investigative Use

- 9/11 Investigations
- Kidnappings
- Child pornography – Innocent Images
- Many others including phishing, botnets, pharming, IPR, and Internet fraud related investigations

Questions ?