APWG

Data Fusion Initiative

Draft Agenda – REV 1.1/PFC – March 4, 2008
DFI Mustering Meeting
Heathrow, London UK
March 26, 2008

Forensic data sharing is often held out as an imperative for countering ecrime. Yet this axiom is usually proffered with little elaboration of the persistent barriers to effective data collaboration, the kind that would help automate responding to ecrime to the same level of alacrity that ecrime gangs exhibit when actually committing their crimes.

With initiatives at the European Commission and the Council of Europe to organize policy around electronic crime response under way and data sharing initiatives being developed within industry groups in the US, the APWG and its correspondents have an opportunity to help forge data sharing infrastructure and protocols and negotiate some of the obstacles to effective forensic data sharing.

The AWPG Data Fusion Initiative Mustering Meeting at the Heathrow Radisson on March 26, 2008 will examine common forensic needs for law enforcement and responders; consider the technical dimensions of establishing a globally accessible data sharing and data fusion infrastructure; discuss the data usage governance instrumentation such as user agreements that may need to be established among forensic data traders; and, finally, examine the legal and regulatory frameworks that will have to be negotiated in order for forensically potent data to move between responders across jurisdictions and regulatory frontiers.

This is a draft agenda organized with suggestions from a number of the DFI members that will be updated before the meeting at Heathrow. If you have suggestions, additions and amendments, please forward them to Peter Cassidy at pcassidy@antiphishing.org. If you have working papers that could help inform these discussions before the meeting, please send them to the Data Fusion list. If you want to be on that list, please ask Foy Shiver at fshiver@antiphishing.org to add you.

Introductions and Orientation

Exposition of essential problem statement(s)
Mapping of solution vectors for shared resource development

- Data Reservoirs and Technologies
- Governance Agreements
- Legal and Regulatory Interpretations

Forensic Imperatives and Common Forensic Needs

Actor (Individual and Group/Syndicate) Identification and Reporting
Vetting and Reporting mechanisms
Use-case driven data collection
Fast-Flux – Automating data capture
Common Data Formats – IODEF and eCrime Extensions

Inventory of Data Repositories Under Development

UK banks IP cash-out DB
NCFTA DBs (TBC)
APWG Repository and UBL
TBD/TBA

Inventory of Potential Forensic Data Resources

Sandboxes
Malware collectors
DNS Replication Services
Fast Flux Pumps
Botnet Specifics
IXP Traffic Instrumentation
TBD/TBA

Tools for Automating Capture & Processing of Forensic Data

Automated Tools for data analysis:

- Scripts for IP geolocation, Whois data collection & Fast-Flux data collection

Building the universal e-forensic data kitbag
TBD/TBA

Data Usage Governance Instrumentation

TBD/TBA

Negotiating & Neutralizing Legal and Regulatory Barriers to Forensic Data Sharing

US (TBD)
Europe
EU Data protection laws and comparison to individual nation data laws
Evidentiary requirement of source disclosure
TBD/TBA

Infrastructure Planning

Mapping requirements to establishment of a data sharing infrastructure and/or establishment of federating protocols to interactively share data as needed, required and requested by forensic correspondents.
TBD/TBA

MEETING LOGISTICS

Date: 26 March 2008
Time: 10:00 - 15:00
Place: Henley's Salon, Heathrow Radisson Hotel
http://www.radisson.com/londonuk_heathrow