Working Group Notes 14 March 2018, ICANN61 F2F

DT7 Criminal Investigation/DNS Abuse Mitigation Investigation, Notification, and Reputation – Slide 11

- Answers introduced by Marc, noting limited participation of DT7 members in drafting answers
- Overall there are two paths: investigate a possible criminal or contact a possible victim
- During investigation, the entity to be identified is whomever is controlling the DN – that may not be the rightful owner of the DN
- During investigation, may also be appropriate to contact the registrar, reseller, or privacy/proxy provider to identify the possible criminal engaged in the activity or abuse
- During notification, the primary objective is to inform the possible victim; the secondary objective is enabling mitigation of the activity/abuse
- Page 1 Question 2 of DT7 answers: Objective should include reputation?
- How is Question 3 helpful for this purpose? May describe any obligation on response (or lack thereof). May also describe possible benefits to data subjects.
- Were these definitions informed by jurisdiction and limitations imposed by laws in certain jurisdictions? No – application of purposes would depend on jurisdiction and policy, which the drafting team considered outside its remit when simply describing the purpose
- Criminal activities should also include hate crimes, infringement of civil liberties, etc. – these should be noted to ensure consideration during deliberation of this purpose
    - What constitutes criminal activity varies from one jurisdiction to another
    - For example, blasphemy vs. freedom of speech
    - What kinds of activities should be pursued through this purpose vs. who should have access to data for this purpose vs. consent given to collect data for this purpose
    - This purpose should focus on providing a mechanism to be used in jurisdictions, for activities, where it is appropriate
    - What do we do when law enforcement is “bad” and criminal activity is “good”?
        - Being able to notify a registrant that their DN has been compromised is clearly useful
        - Being able to use reputation scores to deter abuse and crime is good

- Where we disagree is in use of registration data to investigate criminal activity
- Legal processes for accessing data for this purpose will be determined by laws, not policy
- For clarity, this purpose should be titled “Criminal Activity Mitigation and DNS Abuse Mitigation” (or Investigation of Criminal Activity and DNS Abuse, Notification of…, etc.)