**Proposed Categorization**

I have used the staff categorizations as my starting point. There is not a huge difference between NCSG and Staff categorization of Group 1 and 2 / Category A and B respectively. Based on our discussions Thursday it would be best for us to agree that in Category A/Group 1 we are talking about official or sworn LEAs and in Category B/Group 2 we are talking about investigations by either non-state actors or governmental or quasi-governmental agencies that are not LEAs, such as CERTs. The distinction between LEAs and other actors, as we have established in our discussions, is a critical distinction because it affects applicable law and the way the balancing test might be conducted. This would result in the following two groups (I will use staff’s Category X notation rather than NCSG’s Group X):

|  |  |
| --- | --- |
| **Group 1:**Criminal Law enforcement/national or public security | LEA 1, LEA 2, IP 1, IP 2 |
| Group 2: Non-LE investigations and civil claims | BC1/2, BC 3, BC 5, SSAC 2, SSAC 3, ALAC 2 |

I have eliminated ALAC 1, SSAC 1 and BC 9 from these groupings for reasons explained below.

The Staff category “commercial” did not make sense to a lot of people and should be eliminated. It consists of 2 use cases, one devoted to M&A due diligence (BC 6) and the other to issuance of digital certificates (BC 8). BC 6 confusingly combines two distinct needs: a need to contact the domain owner to see if they want to sell it, and a form of validation (an acquiring company wants to know whether the domain is really owned by the company they are acquiring). BC 8 is about validating, for the purpose of issuing SSL certificates. The staff categorization simply does not constitute a coherent category. BC 8 is more properly grouped with ALAC 1 and BC 9, both of which are using the domain to validate some identity. BC 6 is really two use cases, not one. The element about validation should be grouped with other validation cases, and the “contact registrant” should be grouped with other use cases based on an alleged need to contact the registrant (BC 7, SSAC 1). So in this case the NCSG proposal is much better and I would propose we keep these two categories:

|  |  |
| --- | --- |
| Group 3: third party validation | ALAC 1, BC 8, BC 9 |
| Group 4: Need for redacted data for a third party to contact registrant | BC 6, BC 7, SSAC 1 |

The staff category “Intellectual property” is not needed because IPR holders are just civil claimants or investigators. As most of the use cases fit neatly under Group 2. The URS/UDRP use case is different because it is not part of an investigation it is part of an adjudicatory process, so it is best to treat it as a stand-alone case.

The remaining staff category, Category E “Domain name maintenance,” which combines BC 4 and BC 7, does not make a lot of sense. BC 4 is about the domain registrant accessing *their own* information, whereas BC 7 is about *third parties* wanting to contact the domain owner to resolve technical issues. BC 7 obviously should be grouped with SSAC 1, which says almost the exact same thing about contacting the registrant to resolve operational issues. And there is also an element in BC 6 that asserts a need for third parties to contact the registrant to buy the domain. So here again, the NCSG categories work better. BC4 is really a unique, stand-alone use case that does not need to be grouped with any other, and BC 7 belongs in Group 4. So that gives us:

|  |  |
| --- | --- |
| Standalone use cases | IP 5, BC 4 |

To conclude, I would summarize the following compromise grouping that takes elements from both the NCSG and Staff groupings:

|  |  |
| --- | --- |
| **Group 1:**Criminal Law enforcement/national or public security | LEA 1, LEA 2, IP 1, IP 2 |
| Group 2: Non-LE investigations and civil claims | BC1/2, BC 3, BC 5, , SSAC 3, ALAC 2, IP 3, IP 4 |
|  |  |
| Group 3: Need for redacted data for a third party to contact registrant | , BC 7, SSAC 1 |
| Group 4: Consumer protection, abuse prevention, digital service provider (DSP) and network security | SSAC 2, BC 9 |
| Group 5: Registered Name Holder consent or contract | BC 4, BC 6, BC 8, IP 5 |
| Standalone use cases | ALAC 1 |

The original groupings are on the next page for reference.

**Staff**

|  |  |
| --- | --- |
| **Category A:**Criminal Law enforcement/national or public security | LEA 1, LEA 2, IP 1, IP 2 |
| Category B: Non-LE investigations, consumer protection, abuse prevention and network security | BC1/2, BC 3, BC 5, BC 9, SSAC 1, SSAC 2, SSAC 3, ALAC 1, ALAC 2 |
| Category C: Intellectual Property | IP 1, IP 4, IP 5 |
| Category D: Commercial | BC 6, BC 8 |
| Category E: Domain name maintenance | BC 4, BC 7 |

**NCSG**

|  |  |
| --- | --- |
| Group 1: Criminal law enforcement | LEA 1, LEA 2, IP 2, IP 3, BC 1/2, SSAC3 |
| Group 2: Civil law enforcement | IP 1, IP 4, ALAC 2, BC 3, BC 5 |
| Group 3: Random forms of validation | ALAC 1, BC 8, BC 9 |
| Group 4: Need for redacted data to contact registrant | BC 6, BC 7, SSAC 1 |
| Standalone use cases | IP 5, BC 4 |

**IPC**

|  |  |
| --- | --- |
| LEA Cases | LEA 1, LEA 2, IP 2, IP 3 |
| Trademark, Copyright, Phishing / Malware, Network attacks | IP 1, IP 4, SSAC 1, SSAC 3 |
| Social media, search engines, messaging services, online buyers | BC 9, ALAC 1 |

**BC**

|  |  |
| --- | --- |
| LEA investigations of Criminal Activity | LEA 1, LEA 2, IP 2 |
| Investigation/prevention/mitigation /resolution/legal action of criminal/civil fraud by non LEA | BC1/2, BC 3, SSAC 1, SSAC 3 |
| Reputation/Integrity Establishment for Internet Infrastructure, Services & Platforms | BC 9, SSAC 2, BC 8 |
| Consumer Protection | ALAC 1, ALAC 2 |
| IP Legal claims / investigation / defense | IP 1, IP 4, IP 5 |
| Domain registrant uses | BC 6, BC 4 |
| Contacting registrants to resolve issues or legal claims | BC 7, BC 5 |

**LEGEND**

|  |  |
| --- | --- |
| LEA 1 | Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a non-local data controller. |
| LEA 2 | Investigation of criminal activity against a victim in the jurisdiction of the investigating EU LEA requesting data from a local data controller. |
| SSAC 1 | When a network is undergoing an attack involving a domain name, and the operator(s) of that network need to contact the domain owner to remediate the security issue (DDOS, Botnet, etc.) |
| SSAC 2 | Determine “Reputation” of domain name and/or elements associated with domain name registrations. |
| SSAC 3 | Investigation of criminal activity where domain names are used.  Typical specific example: phishing attack. |
| IP 1 | Trademark owners requesting data in the establishment, exercise or defense of legal claims for trademark infringement |
| IP 2 | Investigation of criminal activity against a victim in the jurisdiction of the investigating LEA requesting data from either a local a non-local data controller. |
| IP 3 | Investigation of criminal activity in the jurisdiction of the investigating LEA requesting data from either a local a non-local data controller. |
| IP 4 | Copyright owners requesting data in the establishment, exercise or defense of legal claims for copyright infringement |
| IP 5 | Providers requesting access required to facilitate due process in the UDRP and URS |
| BC1/2 | Initial investigation of criminal activity against a victim and/or secondary victim where domain names are used in the commission of the crime |
| BC 3 | Identify owner of abusive domains and other related domains involved in civil legal claims related to phishing, malware, botnets, and other fraudulent activities |
| BC 4 | Maintaining the domain name registration by the Registered Name Holder |
| BC 5 | The establishment, exercise or defense of a legal claim involving a registrant of a domain name |
| BC 6 | M&A name portfolio due diligence or purchase of domain name from bankrupt entity or other seller |
| BC 7 | Contacting the Registrant to resolve a Technical or Operational Issue with a Domain Name |
| BC 8 | Help a certification authority determine and validate the identity of the entity associated with a domain name that will be bound to an SSL/TLS certificate |
| BC 9 | Search Engines, Messaging Services & Social Media Platforms seeking to confirm the authenticity of businesses advertising or Posting News on its Platform |
| ALAC 1 | Online buyers identifying and validating the source of goods or services/ Internet users validating the legitimacy of an email or a website to protect themselves |
| ALAC 2 | Consumer protection organizations |