

CATEGORY F - REVEAL

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
2. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?
3. What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger a reveal?
4. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
5. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
6. What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?
7. What specific alleged violations of the provider's terms of service, if any, would be sufficient to trigger publication of the registrant/owner's contact information?
8. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?
9. What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?