Privacy is an integral part of our society. However, openness and availability of information equally important for scientific advancements. The fine line between ethical responsibility and evolving re-computational practices should be clearing defined. Re-Computation (ER) is an initiative by [CreditsHere] academic community to enable the early stage researchers stand on the should of giants while avoiding to reinvent the wheel. Academic Re-Computation (ARC) will allow researchers to move forward with given results while integrating the relevant domain specific knowledge in the existing solution.

ARC emphasis on set of practices for any given experiment which include software (application programming) as a source of conclusion to the discussed problem. This includes software {OS/Platform/user-apps?}, dataset, parameters, pre/post conditional legends and documentation to re-produce the results while executing the experiment. Published work should serve ultimate documentation of the conducted experiment, unless because of technical reasons such as format (space/style) and straying from main idea would result distraction to reader. In this case, detailed information should be provide in terms of index, references or web links to obtain scripts with processed data.

Ethical and privacy concerns are the way points how ARC will be implemented, we summarize and discuss these issues in following three categories.

- Disclosure or Identity Theft: Discloser is a privacy threat which produces back-track to original experimental source. The identity of users must and should be deframed while providing pseudo-user. In significant cases we emphasis any experiment that uses or make use of human intervention part of experiment in direct or remote sense. Published ARC should follow the predefined user rights [User-Acceptance-agreements]. Proven data mask techniques should be used to ensure that no adversary would be able to track the users. Data mask is a technique which allows to change the data without changing its original format. The used mechanism to mask the data should include complete set of data and as well individual and independent dataset.

- Integrity: The integrity threat involves intentional or unintentional change in data leading to sensitive information. The details provided in ARC should not lead to identification and sufficient mechanism to obscure the identities must be fundamental practise before sharing the user information. Provided data should never include sensitive and personal details in any forms.

- Replication: ARC should provide means to reproduce the results while cloning the data and parameters involved in experiment. But, it is important that replication should not imitate to possible user scenarios. For example, names of users from social data replaced with random number generator but other delicate details left intact. Researchers should ensure that replication of data should not lead to real identity or Intellectual property infringement.