

Data Privacy Agreement
Cooperative Association for Internet Data Analysis
University of California, San Diego

The purpose of this document is to outline the general expectations of all users given access to sensitive network data stored on or collected from any CAIDA machine. The current definition of sensitive is information related to IP addresses that can be mapped to entities. This definition may be expanded as need arises. Information about this can always be obtained from CAIDA PIs. **CAIDA senior staff have the authority to disable logins immediately and take additional disciplinary action, including termination of employment, for failure to comply with this agreement.** In general, access to sensitive network data does not give you any additional rights, only responsibilities.

Usage of sensitive data must be limited to analyses that cannot be completed using desensitized data. Access to traces will be approved on a case-by-case basis provided:

- (1) The analysis can produce some tangible benefit to the community.
- (2) The specific scope of the analysis is outlined in a written statement and approved by CAIDA. Sensitive data will not be used for purposes outside of this scope.
- (3) All research results will be made public.

Information gained from sensitive network data is **privileged**. You are personally responsible for ensuring that any information you may obtain from sensitive network data is not used by yourself or anyone else in any manner that might violate the privacy of CAIDA, the organization that supplied the data, or end users.

In particular, data collected from passive monitors at UCSD fall under the purview of the University of California Electronics Communications Policy (UC ECP document). **Initial here** ____ that you have been given copy of the UC ECP document, either in printed form or a URL, and have read and agree to abide by section IV, Privacy and Confidentiality. (<http://www.ucop.edu/ucophome/policies/ec/>)

At no time will any sensitive data be removed from the local machines that have been specifically configured and approved by CAIDA to store this data. Any reduced data generated from sensitive network data must not contain un-encoded IP addresses, AS numbers, or other information that would allow a third party to determine the specific source, destination, or content of the network traffic.

Information obtained from sensitive data will not be used as part of any active measurement without obtaining approval from CAIDA. Specifically, host addresses extracted from sensitive data will not be used as the targets for any probing without prior approval. For the purposes of this section, attempts to contact administrators or owners of hosts are considered an active probe.

CAIDA reserves the right to review all results using CAIDA data before they are submitted for publication for the purposes of determining whether or not the published data constitute a privacy infringement. If such an infringement is found, CAIDA will specify the nature of the problem, and list specific modifications to the results that will alleviate the problem. I agree that I will not publish any results obtained from CAIDA's sensitive network data without obtaining prior approval. Use of such data or other CAIDA resources requires that CAIDA be credited, e.g., in publications.

I understand and will abide by the above terms and conditions. If the propriety of any situation is unclear, I will ask for clarification from CAIDA PIs rather than making assumptions. I understand that my access to sensitive network data may be revoked if the terms and conditions are not adhered to.

Login: _____

Printed Name: _____ Phone: _____

Signature: _____ Date: _____