Privacy Plan

The Center for Applied Internet Data Analysis (CAIDA) has more than twenty years of experience in collecting, curating, and analyzing Internet measurement data and is renown worldwide for sharing the raw and derived data with researchers. Over the years, we have proven our unwavering commitment to safeguarding the integrity and privacy of the data we collect.

What information do we collect for IODA-NP project?
To detect and analyze outages, we continuously collect and monitor Internet data from the following three sources: BGP routing information provided by the RouteViews and RIPE RIS projects, Internet Background Radiation (IBR) captured at the UCSD Network Telescope, and active probing of /24 networks performed by CAIDA. None of these data contain any Personally Identifying Information (PII) or represent any privacy risks. BGP information is publicly available. IBR data is one-way unsolicited traffic generated by hosts worldwide due to misconfiguration, malware propagation, DDoS attacks, or other malicious activities; it does not contain any personal communications. Our active probing monitors send probes to random addresses in IPv4 routable /24 networks and simply mark them as responsive or not.

We also use third-party data – WHOIS database – to infer a mapping from Autonomous System (AS) numbers to the organizational entities. The WHOIS service is a free, publicly available directory providing the contact and technical information of registered domain name holders. We do not give access to original raw data outside of CAIDA. Finally, we use commercially licensed and free public IP Geolocation datasets from commercial providers. This data does not contain any PII.

What do we use your information for?
We continuously process the raw measurement data from each source to extract a time series "liveness signal" for various geographic regions and/or Internet Service Providers (AS). Drops of any of those signals below a dynamically predicted threshold constitute an outage event detection and generate an alert. Alerts are recorded and further analyzed to determine the scope and significance of a given event.

How do we protect the collected data?
All CAIDA data is maintained securely on CAIDA servers and accessible only by authorized users. Since we use all these data for various other CAIDA research projects, we do not currently have plans to dispose of the data after the end of this project.

Do we disclose any information to outside parties?
We do not sell, trade, or otherwise transfer to outside parties the raw data that we collect using our own measurement platforms (the UCSD Network Telescope and active monitors), except to trusted researchers for pursuing legitimate research.

We do not give access to original raw WHOIS data outside of CAIDA.

We publish alerts and post-processed aggregated data, which we make publicly available through the IODA web dashboards and APIs and through alert feeds. We commonly release data used in publications as separate packages.

Acceptable Use Policies
Researchers requesting access to CAIDA raw data have to fill in a form online and sign electronically the CAIDA Acceptable Use Agreement (AUA). Our AUA allows the use of data for legitimate research only and establishes the access obligations, use and disclosure restrictions, disclaimers, and limitations of liability governing CAIDA data sets. It strictly prohibits distributing data beyond authorized users, and enforces appropriate privacy protecting de-identification or anonymization for publications. We developed this AUA based on the privacy sensitive data sharing principles formulated in [1].

For sharing our most sensitive datasets, we also rely on a well-established legal framework of the DHS-funded Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) project to implement proper data disclosure controls. Sharing our data via IMPACT allows us to enable access to our data only for vetted researchers in a secure and controlled manner that respects the security, privacy, legal, and economic concerns of Internet users and network operators.

Access to our publicly available datasets is subject to terms of a more permissive CAIDA Acceptable Use Agreement for Publicly Accessible Datasets (Public-AUA).

Contacting Us
If there are any questions regarding this privacy policy you may contact us at data-info@caida.org.

[1] E. Kenneally and k. claffy, Dialing privacy and utility: a proposed data-sharing framework to advance Internet research , *IEEE Security & Privacy*, v. **8,** no. **4**, pp. 31--39, Jul 2010.