International Networks at Indiana University Data Privacy Policy
September 8, 2021
Author: Hans Addleman

International Networks at Indiana University (IN@IU) collects packet header data from the routers and switches comprising the TransPAC and NEA3R networks. IN@IU does **not** capture any user data stored within a packet payload from the network. NetFlow and sFlow data is a sampling of the network traffics packet headers on the networks and can include any of the following elements:

- Source and destination IP address
- Source and destination autonomous system number (ASN)
- Source and destination port
- Protocol (IE: tcp, icmp, udp)
- Size and length of each traffic flow
- Start and end times of traffic
- Router or switch interface traffic transmitted
- TCP Flags
- MTU size

IN@IU uses the above data to assist in troubleshooting, traffic capacity planning, reporting to funding agencies, and research:

- Troubleshooting: Raw netflow data is used by TransPAC and NEA3R network operators to diagnose and solve issues as they present themselves.
- Capacity Planning: TransPAC and NEA3R engineers use this data to plan network augments and routing optimizations.
- Reporting: IN@IU reports high level de-identified Autonomous System top ten talker reports to their funding agency.
- NetSage: IN@IU provides netflow data to the NetSage project in a de-identified state for traffic measurement and visualization as required by the National Science Foundation. More about Netsage can be found at http://www.netsage.global/

IN@IU sampled data is stored by the IU (Indiana University) GlobalNOC and is classified as critical following Indiana University classification guidelines. Appropriate measures to protect this data are practiced by the IU GlobalNOC.

- https://datamgmt.iu.edu/types-of-data/classifications.php
- https://globalnoc.iu.edu/

Netflow records will only be shared in a de-identified or aggregated state. De-identification of data will be performed by truncating all IP addresses to remove at least the last 8 bits for IPv4 or 64 bits for IPv6. This removes the computer/user specific part of the IP addresses leaving only the institutional level addressing. Aggregated data is compiled in such a way so that network activity can not be attributed to an individual user. Researchers may request access to this

aggregated data by emailing the International Research Network Connections Network Operations Center at irncnoc@globalnoc.iu.edu.