MEASURES FOR JUSTICE

Data Repository Best Practices

MFJ recommends that all states identify a state agency to act as a criminal justice data aggregator and repository for data from local criminal justice agencies across the state. The specific agency serving in this function will vary based on state-specific dynamics and the organizational structure of the state criminal justice system. Below are a set of capabilities that a data aggregator and repository agency should have:

1. Uses open web standards. Little use of proprietary technology.
2. Uses security on the transport layer. Website is https (rather than http) even for non-login pages.
3. Uses modern scaling technologies (Tech that allows you to handle large spikes in traffic).
4. Has people on staff that are dedicated to web user-interface coding.
5. Has people on staff that are dedicated to web service ("server-side") coding.
6. Makes data available in machine-readable, open format files (i.e., you can get full datasets without scraping).
7. Makes data available and searchable via modern web APIs (access to data directly through programs, not just by humans going to web pages).
8. Has the capability to aggregate, stitch together and validate the data coming in.
9. Can handle, for example, duplicate, overlapping or missing data and has processes for the rejection and re-transmission of invalid data.
10. Uses standard best practices for data protection and redundancy (remote backups, logging, event detection). If you're interested in MFJ assessing your state's data or want to know more about how to improve data collection, recording, and sharing, please contact us.