Policy
454

Fresno Police Department Policy Manual

Beware®

454.1 POLICY

The policy of the Fresno Police Department is to utilize Beware® to access commercial and public data associated with the address of a law enforcement event while recognizing the established privacy rights of the public. The data can assist members in developing strategies for the successful resolution of emergency incidents; but it is not to be used as the sole reference point in making life-saving decisions. The first responder must continue to rely on their training and experience.

All data gathered by Beware® are for the official use of this department. Because such data may contain confidential information, they are not open to public review.

454.1.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the access and use of Beware®.

454.2 DEFINITIONS

Beware®: a program created by West, Inc. that searches and compiles commercial and public data associated with the address of an emergency event in progress from thousands of data sources. From this information, Beware® identifies people associated with an address; delivering a summary on each within a matter of seconds. These summaries provide names associated with the address, their phone numbers, their nearby relatives and associates along with their addresses and phone numbers, and also criminal records data. Beware® contains data on close to 100% of the adult population, and close to 100% of residential addresses. Both land line and cellular phone registrations to residential addresses are available. Court records are acquired on a daily basis and are available. Often Beware® presents data typically unavailable to public safety, but which could prove highly instrumental in the successful resolution of emergency events.

Personally Identifiable Information (PII): information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

454.3 PRIVACY

The use of public and commercial records in public safety began in the mid-nineties, and has become an accepted and established practice. Criminal records, a specific category of public records, will often reflect data contained in Criminal Justice Information Systems (CJIS). While some may believe the criminal record data in Beware® is CJIS data, it technically is not in that the criminal records were collected at the source (i.e., the county courthouse) by a commercial aggregator and then made available to other commercial providers (such as West, Inc. with Beware®). This data is sourced nationally, which allows Beware® to provide a more complete picture of people involved in an emergency event.

The ACLU has long recognized the accepted use of PII in helping enforce the laws of the country and in protecting our communities. The caution has always been against any unauthorized, arbitrary or capricious use of PII data. To that end, providers of services that use PII must guard against this. Beware® contains a series of privacy processes to guard the PII of our citizens, including the credentialing of all clients and end-users, strict information security environment provisions, continuous monitoring-of-usage processes, and compliance reviews on a scheduled basis.

While US and state statutes allow public safety nearly un-restricted usage of PII data, Beware® suppresses some data elements. Most commercial data providers only provide redacted social security numbers, dates of births and driver's license numbers. In rare cases where Beware® receives un-redacted data, it immediately redacts before any further processing, and discards all

drivers' license data. The information provided by Beware® will not include any type of scoring, color-coding, or public social media postings attributed to individuals. Results will only display an asterisk alongside any name containing criminal history information.

All communications between Beware® servers, data providers, and customer clients is encrypted and protected with HTTPS certificates.

454.4 USE OF BEWARE®

Deploying Beware® in the Real Time Crime Center (RTCC) allows FPD personnel to deliver situational awareness alerts directly to the first responders as they respond to events. These alerts can relate to wanted persons, restraining orders, violent criminal history, etc. Having this information can help guide the response strategy and lead to safer outcomes for all involved. Some examples of this may be to request or wait for additional assisting officers, attempt to call the residence rather than approaching, contacting relatives or associates for additional information, etc. Beware® has been integrated into the RTCC Application, allowing location information to be automatically sent to Beware® when the calls are created in the 911 center, with results returned in seconds directly to the RTCC operators.

RTCC personnel will primarily access Beware® through the RTCC Application. The results will be returned directly to the Beware® tab in the application. This allows RTCC personnel to perform more efficiently, provides an additional level of security and logging, and connects each Beware® query to an event.

Beware® presents data helpful to the first responder in the successful resolution of emergency incidents; but it is not to be used as the sole reference point in making life-saving decisions. The first responder must continue to rely on their training and experience.

454.5 ACCESS

All data will be closely safeguarded and protected by both procedural and technological means. The Fresno Police Department will observe the following safeguards regarding access to and use of Beware®:

- *(a) All user accounts require approval by the Chief of Police or designee before establishment;*
- *(b) User accounts will be limited to members assigned to the Crime Center, with a specific, ongoing need to access the system for the purpose of emergency response, criminal investigations or pre-planned police actions;*
- *(c) All members designated as system users shall receive training and a unique user identification in order to access the system;*
- *(d) End User forms must be submitted by every member who accesses Beware®. The form must be completed, signed, and approved by a Crime Center supervisor prior to gaining access.*

454.6 AUDITS

Use of the system will be audited on a regular, on-going basis by Crime Center supervisors. Additionally, on a long-term basis, the Office of Independent Review (OIR) may perform audits to be included in its quarterly report(s), and an audit of the system will be included in the biennial Video Policing audit. Any modification to agency or user data is logged and tracked. All user usage data is captured and audited with the commercial data providers. The agency receives a full user usage report at the first of each month detailing the activity of all users. All search data is archived for seven years. Unauthorized access to the system, misuse of the system, unauthorized reproduction of data, or unauthorized distribution of data may result in disciplinary action up to and including termination.

454.7 TRAINING

The Crime Center Commander should ensure that those authorized to use or access Beware® receive department-approved training. West, Inc. provides initial and continuous training to public safety personnel in the use of Beware® to ensure that use considerations will always be recognized and optimized.