PAB questions to SDPD 2/12

CellHawk:

1. “This type of data is used in active investigations typically associated with exigent circumstances.” Does this mean you are tracking or trying to find a person or device? What are exigent circumstances?

2. What information is extracted by the tool other than location data?

3. “Data retained in CellHawk can be accessed by analysts working for Hawk Analytics.” This is a potential risk since the analysts may pool information and create AI models. Are there any regulations governing or limiting the access and data-use by Hawk Analytics?

CPClear:

1. “When a user logs in, they must choose their “Permissible Purpose” for 3 categories:” Does this mean that they make a choice in each of these categories, or that they pick one of these 3 categories?

2. “Use in connection with a non-commercial purpose.” I don’t follow what this has to do with Voter’s permissible purpose or with the PD.

3. “Notification that the user is accessing a restricted information system. Notification that system usage may be monitored, recorded and subject to audit.” Who is notified here? How is the notification information audited or checked for access for un-allowed purpose?

4. Is there any limitation in what kinds of queries can be made, and what information sought, from CPclear in a particular investigation, something ensuring the search stays within the scope of the investigation?

5. “Information gathered by a user is only a pointer system. The individual user validates the authenticity of the information through the appropriate custodian of records, typically a law enforcement agency, or if necessary, through another non-law enforcement service provider by means of a search warrant.” I don’t follow this. What is a pointer system?

Berla:

1. “The acquisition and analysis is typically conducted pursuant to a search warrant authorized by a Superior Court Judge.” Does the search warrant limit the scope of the data acquisition and analysis, for example that certain vehicle systems can be accessed but not others? If so, how is this restriction on scope enforced?

OffenderWatch:

1. What is the criteria for sharing sex and arson offender data with the National Sex Offender Public Website (NSOPW)?

Realquest:

1. What checks are in place, if any, to verify that only authorized personnel have Realquest access?

FaSTR
Grayshift GrayKey
Magnet Forensics AXIOM
Cellebrite UFED

Universal comments:

1. The use policies do not use limited lists; instead they use open language (e.g., "when proper authority, such as a search warrant or consent"). For all use policies, please use exclusive language. Otherwise, this indicates that there are other uses that are not listed. If there are other uses, please list those. Prohibited uses should also be stated.
2. Please update all use policies to provide more information about access to the data, not merely access to the software. The use policies should state who can request an extraction/analysis and who has access to the results of the extraction/analysis. It's also unclear where extracted information is stored.
3. Please update all use policies to provide information about who does audits of PD uses of these technologies and who has oversight of these uses. The current statements do not specify any auditing or oversight requirements except for logging of access.
4. The training, auditing, and maintenance sections of the use policies do not provide any meaningful information. Please update all to reflect who specifically is responsible for these and how they are conducted.

GrayShift and Cellebrite:

1. Is there a way to limit what is extracted (e.g., based on content, date/time, specific individuals)? Or is everything extracted (all or nothing extraction)? If all or nothing, do authorizations put any limits on what can be accessed once extracted?
2. Who has access to the results of the extractions? Please update the access sections to specify.
3. Which types of social media platforms are extractable? Please update the data collection sections to specify.
4. What specific trainings are required for use of these technologies? Please update the training sections to specify all trainings, to include training on the use policies.
5. Approximately how many times a year are these technologies used?

FaSTR:

1. DNA information (markers, etc.) is personal data. That is precisely the intent to build a DNA profile that identifies a person. Please update the use policy data collection section to specify that personal information is collected.
2. Is this information compared against a database of genetic information or compared to a model? If so, please update the use portion of the policy to specify that this is an intended use and specify what databases or models FaSTR uses to create profiles or compare with profiles of other people.

3. Why is this information maintained indefinitely?

Magnet Forensics AXIOM:

1. Similar to the question about FaSTR, is the cell phone information compared against a database or model? If so, please update the use policy to specify.