1 Sensitive Data Working Group

1.1 Purpose

Describe the problem and formulate testable requirements for the various issues surrounding "sensitive" data. What legal, moral, ethical, confidential, political, and social problems can occur with the collection, aggregation, display, and export of the data collected by mobile devices that FAIMS is developing? What do bad actors look for in archaeological data? How can we protect against them?

The working group should also discuss and provide direction on any other aspect of the FAIMS project relevant to the capture, management, or publication of sensitive data.

1.2 Scope

FAIMS is aware that many categories of archaeological data collected in the field may be sensitive, personal, or confidential in nature. FAIMS is asking this group to define the kinds of data should be considered sensitive, and to articulate approaches to recording such data. FAIMS also requires guidelines and strategies for managing, archiving, sharing, and digitally publishing sensitive data.

1.3 Topics to Consider

a. What kind of sensitive data will we be capturing with mobile devices?

    a. What specific components of the data are sensitive? Who should it be protected from?

    b. What component of the data should be shared? What level of sharing control should it have in the best of all possible worlds? What could go wrong with that level of sharing control?

    c. What makes this data sensitive beyond its individual components?

    d. What sensitive data is routinely recorded?

    e. What edge cases should we cover?

    f. How have previous systems failed you?

b. How will people want to interact with this system?

    a. Do we want to provide all these methods?

    b. What other methods do we want to provide?

    c. What are the different use cases for adding data, editing data, accessing data, and searching data?

   d. What preparatory actions does the system need to support?

   e. How can the system promote and require external analysts to maintain adequate protection of the data?

      a. Will people actually *use* this feature, or will they work around it?

      b. How would an analyst actually interact with the data?

c. How will bad actors want to interact with the system?

   a. Do we want to presume good faith?

      a. Are all actions allowed unless forbidden, or are all actions forbidden unless allowed?

      b. What general uses cases for classification are there?

   b. What audit capabilities are necessary?

d. What aggregations are necessary to prepare data for bulk export?

   a. Do these aggregations protect the sensitive data?

      a. Why?

   b. How could a bad actor de-anonymize these aggreations?

      a. Are the detail-tradeoffs worth the level of protection afforded?

      b. Is this just complying with statutory regulations without providing true anonymity?

e. How would sensitive data be useful to other archaeologists in the field?

   a. How would they authenticate themselves?

   b. How would they access it?

   c. How would bad actors use this as an attack vector?

   d. How have you used other sensitive data? How did you access it? What sucked about the access method?

f. Is there any consistency in rules about sensitive data? What's the most ironic rule "trap" you've experienced in this regard?

1.4 Expected Outcomes

a. List of (say) 10 types of sensitive data, with a brief statement about what makes each sensitive.

b. List of requirements for the recording of sensitive data in the field.

c. List of minimum security and publication requirements for archiving and publishing sensitive data.

d. List of functionality requirements for searching, publishing and sharing sensitive data on the FAIMS portal.

e. Suggestions for tools to be included or developed for the FAIMS portal useful for analysing sensitive data.