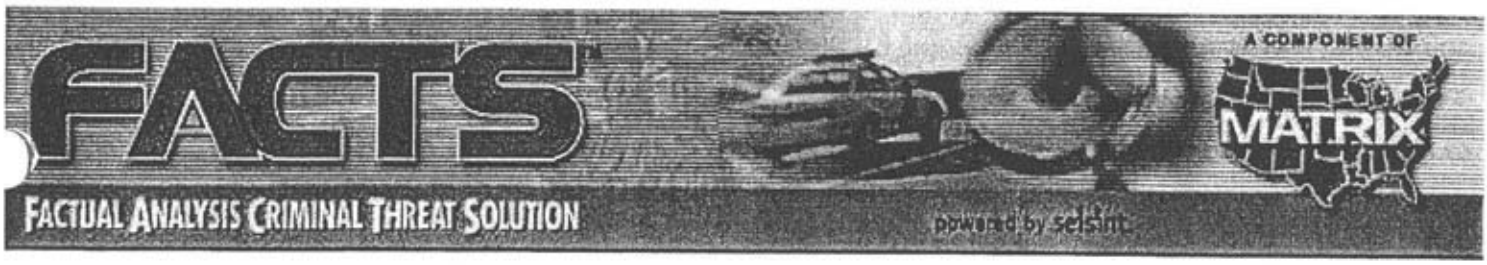


"Where risks appear immediately law enforcement must respond instantly"

Seisint's FACTS™
For
The MATRIX Project

September 29, 2003

Executive Summary

When a child is kidnapped, a murder is committed, or an act of terrorism occurs, law enforcement likely has few immediate details, yet must respond instantly. A Department of Justice study shows that 74% of the abducted children who are murdered, are dead within three hours of the abduction[1]. Individual witnesses may be able to describe a fleeing car, a partial license plate, a description of a suspicious person, or other limited information. Unfortunately, current law enforcement technology does not have the capability to effectively use the reported information to produce investigative results within the critical window to respond. As a result, tragedies occur, cases remain unsolved and significant investigative resources are expended unnecessarily.

Seisint's **F**actual **A**nalysis **C**riminal **T**hreat **S**olution (**FACTS**™), a unique and innovative investigative toolset, solves this critical problem by enabling law enforcement to take incomplete witness accounts and develop leads in seconds, versus manually intensive efforts traditionally requiring days, weeks or months. With FACTS, law enforcement can now instantly and easily search billions of dynamically combined records from disparate datasets with a single query, returning immediate results in easy-to-view and meaningful formats.

FACTS' powerful capabilities raise privacy concerns not unlike the initial computerization of government files, such as vehicle registrations and drivers licenses, from their index card origins. The privacy concerns at that time included questions such as what data was included and why, under what circumstances can it be accessed and by whom. Indeed, these are the questions now being asked about the MATRIX program. Not surprisingly, the answers are the same. Using FACTS, law enforcement has exactly the same access to the same data for the same reasons as they had prior to its invention....only faster. The result is a safer community.

Over the past 18 months, hundreds of law enforcement investigative analysts have proven the unique and innovative aspects of the FACTS solution in the field. Their investigative successes using FACTS show the power of combining Seisint's patent-pending complex query and matching algorithms,

---

[1] *Case Management for Missing Children Homicide Investigation*, . Christine O. Gregoire, Attorney General of Washington & U.S. Department of Justice Office of Juvenile Justice and Delinquency Prevention

weighting formulas specifically designed for law enforcement, and Seisint's delivery speed against billions of data records with law enforcement training and expertise.

The remaining portion of this document contains our detailed proposal to the Institute for Intergovernmental Research (IIR) to provide Seisint's FACTS product in support of the MATRIX program. Seisint is exceptionally proud of the contribution that our non-FACTs information products provide today to over 11,600 law enforcement users nationwide and look forward to extending that relationship to include the MATRIX Pilot program.

Background

Those responsible for our nation's safety and the enforcement of our laws have always been aware of the key role that information has played in the prevention and investigation of criminal activity. The atrocities of September 11th created a new sense of urgency. It is clear that existing legacy systems can no longer keep pace with the overwhelming amount of data that must be analyzed in order to fight the global war on terrorism, and the systemic domestic crime problem.

In the wake of September 11th, and at the invitation of Seisint, a law enforcement working group was formed comprising members of the Florida Department of Law Enforcement (FDLE), the U.S. Attorney's Office (USAO), the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the Immigration and Naturalization Service (INS). This group worked on a collaborative basis with information technology experts at Seisint in an effort to assist in the identification of the yet unknown terrorists.

This working group formed a unique partnership between the multiple federal and state law enforcement agencies and private industry during a time of national crisis. The cooperative effort brought together decades of real-world law enforcement experience and world renowned information technology experts for a common goal — our collective security. During this effort, Seisint provided unparalleled access to both its proprietary data supercomputer technology platform and its data repository of billions of public and commercially available records. The unique insight created by experience and technology, coupled with the resources provided by Seisint, allowed law enforcement to validate Seisint's premise of Factual Data Analysis™: When enough seemingly insignificant data is analyzed against billions of data elements, *the invisible becomes visible*.

The working group contributed useful data to multiple ongoing investigations. The successes achieved and the information sharing lessons learned from this unique experience became the genesis for the idea behind the Multi-state Anti-Terrorism Information Exchange (MATRIX).

After six months of initial work done at Seisint, members of the working group returned to their respective offices to continue their agencies' efforts against terrorism. The FDLE, however, continued to work with Seisint to pursue the ideas and concepts learned during that time, extending the idea of Factual Data Analysis™ beyond terrorism investigations to more traditional crimes. With continued support and resources provided by Seisint, the concepts and ideas were transformed from raw data supercomputing power and sophisticated database queries, to an actual working system called FACTS, known to FDLE as the Florida Crime Information Center Plus or FCIC+. The FCIC+ system extended the power of Factual Data Analysis™ by creating a dynamically integrated database of Seisint's billions of public and commercial records with five of Florida's existing data files: Criminal Histories, Drivers' Licenses, Motor Vehicle Registrations, Department of Corrections records and Sexual and Violent Offender lists.

The FACTS, a.k.a. FCIC+ has been in use by more than 150 FDLE investigators and analysts for more than 18 months, and has been providing valuable assistance to FDLE's ability to fight crime.

Seisint's FACTS has been in use by more than 150 FDLE investigators and analysts for more than 18 months, and has been providing valuable assistance in FDLE's ability to fight crime. The use of Factual Data Analysis™ from existing data sources has saved countless investigative hours, and significantly improved the opportunities for resolving investigations. The numerous success stories surrounding the FCIC+ system can attest to its effectiveness.

The President's National Strategy for Homeland Security[2], July 2002 highlights the foundational role of information sharing to our homeland security:

> *Information contributes to every aspect of homeland security and is a vital foundation for the homeland security effort. Every government official performing every homeland security mission depends upon information and information technology. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Today, there is no single agency or*

[2] National Strategy for Homeland Security, Office Of Homeland Security, July 2002 http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

computer network that integrates all homeland security information nationwide, nor is it likely that there ever will be. Instead, much of the information exists in disparate databases scattered among federal, state, and local entities. In many cases, these computer systems cannot share information—either "horizontally" (across the same level of government) or "vertically" (between federal, state, and local governments). ..... It is crucial to link the vast amounts of knowledge resident within each agency at all levels of government.

The National Strategy calls for a "system" with the power already demonstrated in the field by Seisint's FACTS. The Office of Justice Programs, U.S. Department of Justice, initiated funding for the MATRIX pilot, a proof-of-concept, state initiated and state governed project. The MATRIX pilot project was initiated in response to the increased need for timely information sharing and exchange of terrorist-related information among members of the law enforcement community around the nation. The MATRIX project leverages and integrates Seisint's existing data technology, proven in the State of Florida, to provide a new capability to assist law enforcement in identifying and analyzing terrorist and other criminal activity. MATRIX then enables the information to be appropriately disseminated to law enforcement agencies nationwide in a secure, efficient, and timely manner[3]. Thirteen states are participating in this pilot project with the aim of eventual expansion to all 50 states.

The Challenge:

The Office of Homeland Security[4] set forth the following vision:

"We will build a national environment that enables the sharing of essential homeland security information. We must build a 'system of systems' that can provide the right information to the right people at all times. Information will be shared 'horizontally' across each level of government and 'vertically' among federal, state and local governments, private industry and citizens. ..... We will leverage America's leading-edge information technology to develop an information architecture that will effectively secure the homeland"

The MATRIX challenge is to provide just such a "system of systems" that enables law enforcement to share information across states and produce investigative leads within the critical window to respond. This challenge involves searching and analyzing 10.8 billion records of data in seconds.

---

[3] http://www.iir.com/MATRIX/overview.htm

[4] National Strategy for Homeland Security, Office Of Homeland Security, July 2002 http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf

The Solution

Seisint has a proven commercial track record in solving this type of large-scale complex data management problem. Today, **F**actual **A**nalysis **C**riminal **T**hreat **S**olution (**FACTS™**) is delivering to law enforcement the ability to search billions of dynamically and seamlessly combined records from disparate datasets with a single query, returning immediate results in easy-to-view and meaningful formats.

Seisint's FACTS delivers the two key capabilities critical to the long-term success of MATRIX:

1) The Data Access Capability
    a. The ability to search billions of records from disparate datasets and return results to large complex queries in seconds;
    b. A reference data repository providing comprehensive public records and commercially available data sources; and
2) An interactive investigative user interface with intuitive analysis and data presentation capabilities.

THE DATA ACCESS CAPABILITY

FACTS delivers immediate results to queries by dynamically combining Seisint's reference repository of more than 7 billion records of public and commercial records gathered from thousands of locations, with 226 million records from five separate state databases. The five state databases include the driver's license, vehicle registration, criminal history, sexual and violent

offender, and department of corrections records. The 13-state MATRIX Pilot program requires a solution that supports immediate results on queries against 8.4 billion records, with a 50 state rollout supporting 10.8 billion records. The aggregate size of all of the data exceeds 23.4 terabytes, or said another way, 23.4 trillion characters of text. In fact, Seisint's largest Data Supercomputer installation delivered to-date has the processing capacity to run complex queries against 85.5 terabytes of data, the equivalent of 30.8 billion records, with immediate results. We believe that Seisint's patent pending data technology supporting FACTS is truly the "system of systems" that the Office of Homeland Security envisions.

A FACTS query is the equivalent of searching a room full of file cabinets containing 10.8 billion index cards in no particular order, with each card containing 2,100 characters of text. FACTS delivers on this Factual Data Analysis™ promise: when enough seemingly insignificant data is analyzed against billions of data elements, *the invisible becomes visible*. To provide perspective on this data challenge, it is helpful to illustrate this data challenge in the context of a real world example.

This illustration does not depict an actual case

A 5 year-old girl was reportedly abducted at 123 Any Street, in Los Angeles, CA. A witness account provided the following incomplete description of the vehicle and the abductor

The Vehicle:	Type	"Pickup"
	Make	"Ford"
	Model	"Did not know"
	Color	"Dark color"
	Year	"Newer"
	License Plate Number	"Saw a 'T' somewhere in the plate"
	State	"It was not a California license plate"
The Subject:	Race	"White"
	Hair color	"Looked dark brown or black "
	Height	"Between 5' 11" and 6' 2"
	Weight	"180 – 200 lbs"

Law enforcement has 3 hours to find this 5 year-old girl before the missing child report likely becomes a murder investigation. This is a search for the proverbial needle in the haystack--- except the haystack is on fire.

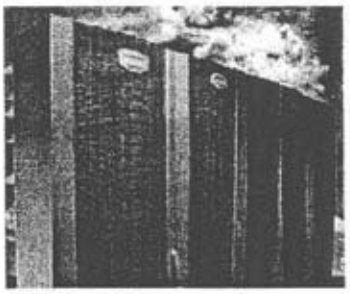
The objective is to compile a photo lineup of likely suspects for review by the witness within the narrow window to respond. This requires a high speed search to assemble the driver's license photos of all persons matching the partial description of the subject, **AND** who own a vehicle matching the witness account, **AND** who have a criminal past that involves child sex crimes regardless of jurisdiction **AND** who today live or have ever lived within 30 miles of the Los Angeles abduction scene.

... when enough seemingly insignificant data is analyzed against billions of data elements, the invisible becomes visible.

FACTS delivers this photo line-up in seconds.

This real-world scenario is not limited to child abductions but applies to reported threats of terrorism, violent crimes including armed robbery, rape and murder, and non-violent crimes such as theft.

The Seisint Data Supercomputer



At the heart of FACTS is the Seisint Data Supercomputer. Seisint's Data Supercomputer technologies were developed starting in July 1998 from the ground up for loading, linking, querying, and analyzing massive data sets at unmatched speeds. The Data Supercomputer platform, built from commercial hardware components and tied together using Seisint's unique patent pending software layer, enables data fusion and analysis of tens of billions of records in seconds and minutes instead of hours, days, or even weeks. It allows access to the entire raw data sets without index constraints of traditional systems. The Data Supercomputer technology is uniquely positioned to provide leading-edge processing of data at speeds previously unattainable.

For example, in one benchmark test, the Seisint Data Supercomputer was compared to traditional data processing technology. The benchmark consisted of a complex predictive neural network model on a population of 267 million individuals involving billions of linked records. When the customer ran this model on only a subset of the data (50 million individuals) using traditional technology it required 26 days to complete. Seisint's technology completed the entire population in just 6 minutes.

FACTS queries are sent by the application to one of four types of supercomputers; in effect, the program selects the best tool for the job. This is all transparent to the end-user. A fifth type of supercomputer performs the Extract, Transform, and Load functions to create a useful database from dissimilar data sets.

The system is also designed to be scalable to meet an increased demand by adding incremental nodes to the existing system. The linear growth potential provides states with predictable price performance and quality of service.

The following proprietary supercomputer components built by Seisint are used in the FACTS system:

Complex Analysis Engine (CAE)

The analytical supercomputer component is a memory-based massively parallel computer cluster optimized for analytical queries. Using a high performance messaging system, nodes interact with each other to perform their tasks and return results of queries. Nodes store the actual data in memory and query response is frequently sub-second.

Queries that require days to run on traditional indexed data, now can be executed in seconds on a CAE cluster. For example, a job that took 24 days to run on an IBM 3090 mainframe, now executes in 6 minutes.

A job that took 24 days to run on an IBM 3090 mainframe now executes in 6 minutes.

Data Refinery

The Data Refinery supercomputer is a disk-based massively parallel computer cluster optimized for sorting, manipulating, and transforming data. The performance gain compared to state-of-the-art sorting solutions is in the range of 100 times or more.

In order to efficiently feed the analytic engine, a similarly massive parallel approach was applied to the Extraction, Transformation and Load (ETL) process. The net result is that complex sorting, sifting and other transformations can be done 8 to 12 times faster than previously possible. The Enterprise Control Language (ECL) also controls the data refinery, bringing the fusion and analysis of data under the control of one powerful language. The Data Refinery is built to handle massive ETL workloads. For example, a job that took 110 hours to run on a 26-processor Sun UNIX server now executes in 6 hours.

A job that took 110 hours to run on a 26-processor Sun UNIX server now executes in 6 hours.

Rapid Data Delivery Engine

The Rapid Data Delivery Engine is a massively parallel query processing supercomputer, using disk-based indexed datasets and pre-compiled repeatable queries. The Rapid Data Delivery Engine works in conjunction with the Data Refinery and Complex Analysis Engine to deliver approximately 1,000 complex query results per second.

Accurint Database Engine

The Accurint Database Engine drives Seisint's flagship Accurint product and routinely processes several million queries a day. The matching engine employs special fuzzy matching technology that can provide accurate links between records in disparate data sources. This supercomputer component is replicated in the MATRIX Data Center to deliver both law enforcement data housed within the secure environment and commercial and public record data.

Image Server

The Image Server is a specialized massively parallel computer cluster designed to store and deliver images from a massive collection of binary graphics files.

ESP Server

The Enterprise Services Platform (ESP Server) provides the interface layer for the FACTS application to access the supercomputer layer. Since ESP uses the standards-based SOAP protocol, application development is faster and more robust.

ECL Language

In order to streamline the construction of complex queries, Seisint created and uses Enterprise Control Language (ECL), which is an easy to learn, powerful SQL-like language which allows for the creation of virtual attributes, stored query objects, and data definitions. By defining attributes in ECL, and using the supercomputer's speed to derive values on the fly, a new level of flexibility and control is obtained.

The Data Reference Repository

A key strength of Seisint's FACTS stems from the data incorporated in the system. Seisint's dynamically integrated and continually updated proprietary master data repository contains in excess of 7 billion public records from thousands of locations on U.S. individuals and businesses. The associative links, historical residential information, and other information, such as an individual's possible relatives and associates, are deeper and more

comprehensive than other commercially available database systems presently on the market.

Seisint's information products are sold to business and law enforcement organizations for legally permissible uses throughout the U.S. Today, over 11,600 law enforcement personnel access Seisint's reference data repository. The repository is sourced from publicly available sources such as county courthouses. Commercial records are sourced from organizations such as those supplying directory assistance listings.

Seisint does not own or license magazine subscriptions lists, telephone calling records, credit card transactions or credit report trade line data (i.e. credit reports), therefore such data is not provided by Seisint to law enforcement. Under federal law, when such data is required to further a law enforcement investigation, law enforcement must obtain a judicial order (i.e. subpoena) and serve it directly on the organization having or owning such data.

In addition to Seisint's proprietary database, FACTS also includes five data files that historically have been available to law enforcement for decades. These files are provided by each participating state to each other under a strict state-to-state user security agreement.

- **Criminal History** information
- **Department of Corrections** information and photo images
- **Sexual Offender** information
- **Driver's License** information and photo images
- **Motor Vehicle Registration** information.

The following files are currently loaded and accessible in FACTS.

Criminal History

1. FLORIDA
2. GEORGIA
3. PENNSYLVANIA
4. UTAH

Department of Corrections

1. ARIZONA	2. ARKANSAS	3. CONNECTICUT
4. DIST. OF COLUMBIA	5. FLORIDA	6. GEORGIA
7. IDAHO	8. ILLINOIS	9. INDIANA
10. IOWA	11. KANSAS	12. KENTUCKY
13. MAINE	14. MICHIGAN	15. MINNESOTA
16. MISSISSIPPI	17. MISSOURI	18. MONTANA
19. NEBRASKA	20. NEVADA	21. NEW HAMPSHIRE
22. NEW JERSEY	23. NEW YORK	24. NORTH CAROLINA
25. OHIO	26. OKLAHOMA	27. OREGON
28. PENNSYLVANIA	29. SOUTH CAROLINA	30. TENNESSEE
31. TEXAS	32. VIRGINIA	33. UTAH
34. WASHINGTON	35. WISCONSIN	

Sexual Offender (Nov 15th)

1. ALABAMA	2. ALASKA	3. ARIZONA
4. COLORADO	5. DELAWARE	6. DIST. OF COLUMBIA
7. FLORIDA	8. GEORGIA	9. ILLINOIS
10. IOWA	11. KANSAS	12. KENTUCKY
13. LOUISIANA	14. MARYLAND	15. MICHIGAN
16. MINNESOTA	17. MISSISSIPPI	18. MONTANA
19. NEBRASKA	20. NEW HAMPSHIRE	21. NEW YORK
22. PENNSYLVANIA	23. SOUTH CAROLINA	24. TENNESSEE
25. UTAH	26. VIRGINIA	27. WEST VIRGINIA
28. WISCONSIN	29. WYOMING	

Driver's License

1. FLORIDA
2. IDAHO
3. MICHIGAN
4. MINNESOTA
5. MISSOURI
6. NEW MEXICO
7. OHIO
8. OREGON
9. TEXAS
10. WEST VIRGINIA
11. UTAH
12. WISCONSIN
13. IOWA (Nov 15TH)
14. MAINE (Nov 15TH)
15. MASSACHUSETTS (Nov 15TH)

Motor Vehicle Registration

1. FLORIDA
2. IDAHO
3. MAINE
4. MINNESOTA
5. MISSISSIPPI
6. MISSOURI
7. NEBRASKA
8. NORTH CAROLINA
9. NEW MEXICO
10. OHIO
11. TEXAS
12. UTAH
13. WISCONSIN

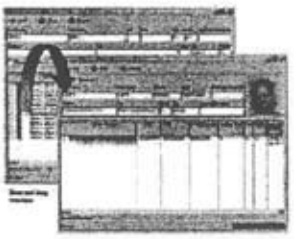
THE FACTS INTERACTIVE INVESTIGATOR'S USER INTERFACE

No two investigations can ever be the same. Each have unique and perhaps never before seen aspects. Systems do not solve crimes, people do. Therefore, t is critical to the success of MATRIX that the user interface is easy to use and supports an investigator's interaction with billions of records of data at the speed of thought. This "conversation" with data requires the ultimate level of flexibility. Specifically, a conversation with massive amounts of data requires the following characteristics.

1) The ability to submit complex queries on indexed AND non-indexed fields without the involvement of IT department personnel.
2) The ability to seamlessly and effortlessly utilize past query results as the input for the next query
3) The ability to represent the query results with a rich set of data visualization tools to enable complex data analysis by the analyst.

FACTS was designed to enable law enforcement to respond instantly when only limited information from eye witness accounts is available. FACTS' interactive user interface brings together Seisint's data supercomputer technology and data reference repository to power hyper-productive analysis that can accomplish thousands of hours of field work in seconds.

The system is simple to operate. Once the user is logged in, all of the search windows work in the same fashion and are intelligently connected to one another. As a query result is sent from one search window to another, the system recognizes what data is needed for the new query, automatically fills in the new search window with the necessary data and then submits the new query.



Identifiers unique to specific inquiries, such as, height, weight, race, sex, vehicle descriptions and geographic data, can be analyzed against the integrated law enforcement database to create investigative tools in real time such as, photo line-ups, target maps and social networking charts.

Basic Query Capabilities

Person Search

Search for a person based on combinations of first name, middle name, last name, SSN, age range, date of birth, address, city, state, zip.

Driver's License Search

Search drivers license registrations based on combinations of first name, middle name, last name, drivers license number, SSN, date of birth, address, city, state, zip.

Motor Vehicle Search

Search for motor vehicle registrations based on combinations of first name, middle name, last name, driver's license number, license plate, VIN, company name, SSN, address, city, state, zip.

Phone Lookup

Search listed phone numbers based on combinations of first name, middle initial, last name, phone number, address, city, state, zip.

Company Search

Search for companies based on combinations of company name, first name, middle name, last name, address, city, state, zip.

DOC Search

Search Department of Corrections records based on combinations of first name, middle name, last name, SSN, DOC#, SID#, address, city, state.

Complex Query Capabilities

Criminal History Search

Search Criminal History records based on combinations of data other than the traditional identifiers such as name and DOB.

Wildcard Search

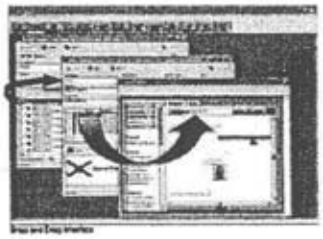
Wildcard searching through the motor vehicle data to run matches on partial license plate tags as well as car makes, models, colors. For example, you can run a query to find all red Fords within a State, which have a "T" as the second character in the tag.

Criminal Data Analysis

Generate leads by searching for individuals who fall within a specified threshold based on indicative data. Where data quality allows, this search combines: Criminal History, Motor Vehicle, Sexual/Offender data, and Department of Corrections data.

Dynamic Chain Search

Select individual or groups of records from the results of one search and use them as input records for another query. This enables dynamic chains of searches. Results are sent to another query by simply using the right-click pop-up menu or by "drag and drop."

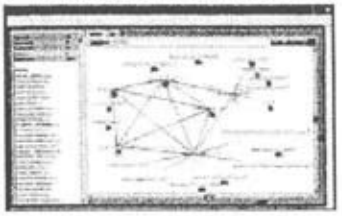


Data Visualization Tools

FACTS' data visualization tools automatically and visually highlight patterns of significance from billions of records in an easy-to-view format.

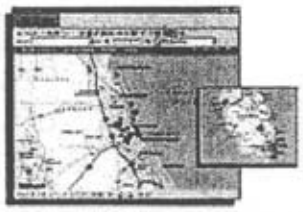
Social Network Visualization

The social network provides data visualization access to the billions of records in the FACTS systems. This feature automatically presents relationships among individuals, addresses, vehicles, and corporations. Users expand links dynamically and develop a continuously evolving network of interrelationships. Features include the ability to determine



previously hidden direct and indirect relationships between and among people.

Geographic Mapping Visualization



Geographic mapping provides a method to visually determine geo-spatial relationships between data. Features include the ability to drag and drop lists of addresses onto a map, the ability to zoom-in to the street and block level, and to drag and drop data from the map into subsequent queries. Microsoft MapPoint 2002 must be purchased and installed separately to access this FACTS feature.

DL Photo Montage Visualization

DL Photo Montage provides a method to view multiple driver's license photos at the same time. Features include the ability to drag and drop query results to display DL photos of the subjects, page forward and backward, individual subject selection, and drill-down queries.

Photo Lineup Visualization

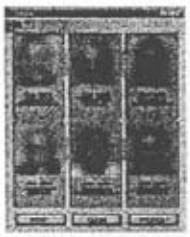


Photo Lineup provides a method to assemble photos of individuals with similar characteristics for the purpose of preparing and printing a photo lineup for witness review. Features include the presentation of 6 images sourced from local diskettes or selected from the DL file using similar characteristics to those reported by the witness such as 25-30 year old, white male, with blue eyes and blonde hair. In addition, photos can be placed in specific positions in the lineup sheet.

Other Capabilities

Search History

The History window provides a display of all prior queries submitted during a session and provides the capability to rerun or save them. This is particularly useful for ongoing investigations because data can be resubmitted against current data that is constantly being updated, revealing information that was previously unavailable.

Printing of Results

Each query window supports the ability to print and save query results.

Comprehensive Reports

Comprehensive reports compiled from all datasets are available for either a company or a person.

Administration

A separate application supports user administration and security. This application allows a trusted administrator to add, modify, or delete user accounts and establish access rights for those accounts.

Recent Announcements and News

This window provides information about new application and data releases. It also provides MATRIX program information.

Coverage Areas Chart

A chart describes the areas covered for a particular search and is available from the Help menu.

User Guide

The User Guide is available from the Help menu.

Seisint's Support of MATRIX

For over two years, Seisint has demonstrated its willingness to dedicate significant time and resources, at no charge, to assisting law enforcement in securing our homeland. Much of the resources are behind the scenes providing operational support and infrastructure including:

- **Data Integration Services** - to handle the receipt, analysis, processing, and loading of the secure law enforcement data.
- **The MATRIX Secure Data Center** - to securely house the machines and data to run the system (including maintenance, capacity planning, and expansion plans).
- **24/7 Support and Help Desk** - to provide individualized services to assist users with the FACTS product and related issues, to ensure safe and accurate data processing, continued enhancements to FACTS, system maintenance, and training.

Seisint's highly-trained specialized workforce is cleared through a Florida Department of Law Enforcement background check. The Florida Department. of Law Enforcement background check consists of a fingerprint-based records check, an intelligence check, a credit check, and an active warrants check (local, state and federal). Only those employees who have completed and passed the background process are authorized to work on the MATRIX project.

The Seisint workforce is broken down as follows:

Data Integration Services Staff
Application Development Staff
System Support Staff (Data Center, IT, Network)
Management and Administration

Data Integration Services

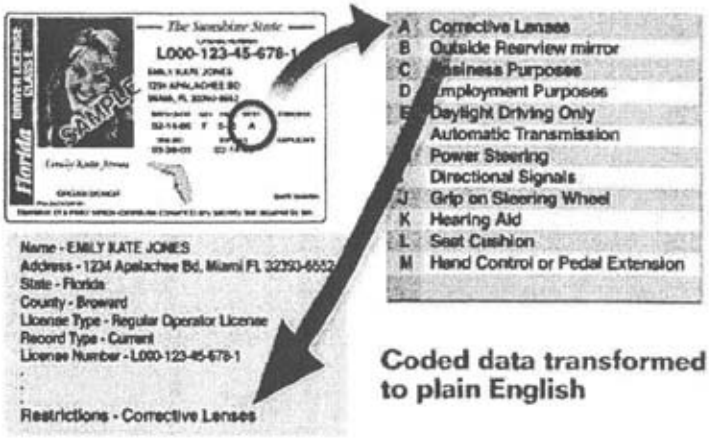
The data incorporated in the FACTS Application is updated continuously. Some datasets are updated daily, some weekly, and some monthly depending on the frequency of the data delivered from the respective source. Seisint uses its proven processes for data receipt, analysis, processing, and loading of the MATRIX data. When a data file to be used by the FACTS arrives at Seisint it goes through the following steps:

1. Physical media containing MATRIX data is received and logged by the FDLE Information Security Officer located at Seisint.

2. The Data Librarian loads data to secure data processing servers. The FDLE Information Security Officer then locks the physical media in a secure room.

3. Data Analysis and Mapping
   - The Seisint data architects analyze the data and map the fields to FACTS formats.
   - The data architects incorporate code tables and lookup tables to properly translate state specific conventions to FACTS conventions, and analyze data relationships to ensure accurate interpretation of data.

4. Data Processing and Extract, Transform, and Load (ETL)
   - The Seisint data processing architects perform a variety of ETL functions on the data to prepare for advanced processing or loading on to the system. These include, but are not limited to:
     - name cleansing
     - address cleansing using current U.S. Postal Service standards
     - standard date transformations
     - standard phone number transformations (including intelligent adding of area codes where missing)
     - data transformations on code fields to plain English



Code transformations are especially useful with state criminal history records. The resulting reports are clear, concise, and understandable, which assists investigators and analysts in their jobs.

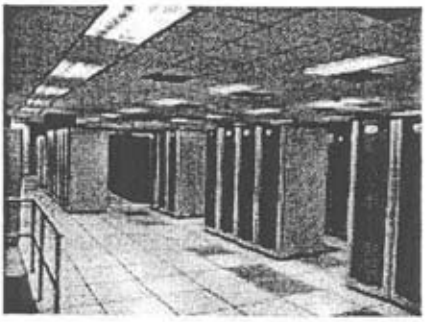
5. Supercomputer Data Processing
   - Following preliminary ETL processing, Seisint regularly loads the MATRIX data onto its proprietary Supercomputer systems. This data is used in standard Seisint data processing models that apply advanced statistics to cleanse, match, and link the data.

6. Following the complete data processing, the data is loaded into the production systems.

7. The FDLE Information Security Officer returns all physical media to a state after receiving the next batch of data from the state.

The MATRIX Secure Data Center

Seisint has created a MATRIX Data Center to be a stable and secure environment to house the data and hardware used by the FACTS system.



System Hardware

The underlying infrastructure behind FACTS runs on a system of supercomputers and their supporting servers, which are all scalable to allow for additional state data.

Data Refinery	The Supercomputer clusters that perform the ETL functions on incoming state data and public record data
Imager Server Supercomputer	Contains driver's license and Department of Corrections images
Reporting Servers	Based on a request for a report on a single search result, reporting servers submit multiple queries to the supercomputers and compile and format reports
Rapid Data Delivery Engine Supercomputer	Supports complex search capabilities
Complex Analysis Engine Supercomputer	Contains state criminal history with associated motor vehicle data for

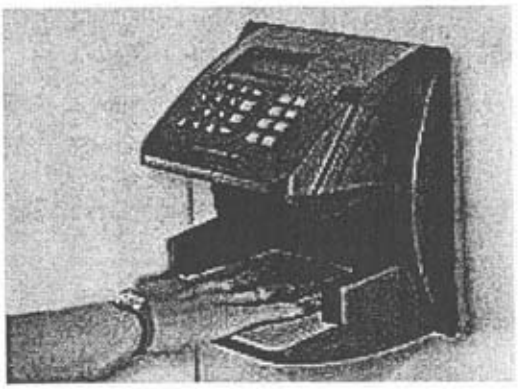
	advanced search capabilities
ESP and ECL Servers	Servers to provide a communication protocol to FACTS and future applications
High Volume Database Search Engine Supercomputer	Redundant processors to provide access to Seisint's data repository and to state data
Logging and Authentication Database servers	Redundant database servers for authenticating users and capturing transaction processing
Isolated and secure network	Contains all network connectivity to interface to RISS network and maintain complete isolation of secure data in an isolated data center

Physical Security

The FACTS hardware components are located in a secure computer room within a larger secure data center, thus it takes advantage of a multi-layered approach to security.

Additional security measures include:

- Biometric Controlled Access
- Motion Detectors
- External Cameras
- Internal Cameras
- Video Recording System
- Lobby Monitors
- Security Room Area
- Security Room Monitoring Station
- Door Locks (Combination and Magnetic)
- Magnetic Reader for Door
- External Entry Barrier
- State-of-the-Art Alarm System



In addition to the security features, security personnel requirements for the FACTS data center include:

- 24x7 Armed Guard
- Security Firm to Provide Armed Response to Alarms
- Management of Security Measures by a Combined FDLE and Seisint Team
- Florida Department of Law Enforcement Oversight of Seisint's FACTS Security Plan

Logical Security Requirements

The following all-purpose security requirements apply to the FACTS system:

- Law Enforcement Control - Dedicated law enforcement personnel strictly control system and data access. Seisint does not add users or control user access.
- User Authentication - Individual user IDs provide authentication and are used to uniquely identify users and control access to FACTS servers on the network. User IDs and passwords do not traverse the network in clear text. The FACTS Administration application (accessible to administrators only) allows the creation of users and groups. Rights given to these groups and users control access to certain portions of the application. This allows function-point access control on either a user or group level.
- Server Access Controls - Access controls are implemented on each FACTS server to restrict access to data and applications.
- Audit Capabilities - All FACTS servers, firewalls, and network devices are capable of providing audit information for purposes of determining suspicious activity or breaches. Each instance of criminal-history or DL Photo access within the application is logged.
- Flexibility - The security scheme can accommodate changes in law as well as new and changing security policies and requirements. Therefore, the security architecture is flexible enough to allow changes without a significant reinvestment of resources.
- Physical Security Measures – Due to the sensitive nature of the data maintained within the data center, additional physical security measures are in place.

Data Security

- Data is physically exchanged among states, not private companies
- The data resides in a secured data center monitored and controlled by law enforcement personnel
- Physical security of the site is strictly monitored and access is permitted via keycard, ID badge, and biometrics
- Advanced firewalls, intrusion detection systems, and other state-of-the-art security measures are utilized
- Each state controls the issuance of its own user ids and passwords, including access rights to certain application functions
- Strict data access and use audits ensure appropriate use of the data

External Network Infrastructure and Connectivity

FACTS has been built to accommodate a variety of connection types. Therefore, it only needs configuration on the network of both the client and the service to make connection complete. The system is designed to be plug-and-play once the client application is installed and connections to the servers are complete.

MATRIX users connect to the FACTS via the secure law enforcement only **Regional Information Sharing Systems (RISS) Network,** which is a federally-funded program administered by the U.S. Department of Justice, Bureau of Justice Administration[5].

The RISS Program is composed of six regional centers that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Typical targets of RISS activities are drug trafficking, terrorism, violent crime, cyber crime, gang activity, and organized criminal activities. Each of the centers, however, selects its own target crimes and the range of services provided to member agencies.

[5] http://www.iir.com/riss/

24/7 Support and Help Desk

To provide support for the ever-increasing user community, and to adequately handle the types of requests that may arise, Seisint performs ongoing troubleshooting, diagnosis, and resolution of problems, including replacing failed hardware components and applying software patches and/or updates where appropriate.

Seisint employs a 24 x 7 Help Desk group to support the telephone call center and email center. The Help Desk support for users is positioned for continued growth as the user community grows.

The FACTS Application support process functions as shown in the table below:

1	**Local State Agency Application Support Team** (handle general questions and issues with Application access and usage)
2	**Local State Agency Escalated Technical Support Team** (handle escalated technical issues such as RISSNET connectivity and network issues)
3	**Seisint Help Desk / Support Team** (handle escalated questions and issues with application functionality & support, access, data transfer, etc)
4	**MATRIX Information Security Officer** (handle escalated questions and issues with application use, access, data transfer, etc)

Seisint shall provide help desk coverage of a designated support telephone number during normal business hours, defined as Monday through Friday, 9:00 am (EST) through 5:00 pm (EST). On-Call Hours are Monday through Friday, 5:00 pm (EST) through 9:00 am (EST), Saturday, Sunday and designated Seisint company-paid holidays.

Problem Resolution

When problems with Application services are identified and reported to the Seisint Help Desk, Seisint shall designate a severity level for each problem as defined below:

Severity Level 1 (Critical Problem)	User cannot access the Application to obtain any information, resulting in a critical impact to operations requiring fast resolution.
Severity Level 2 (Major Problem)	User can access the Application, however a material function is not available.
Severity Level 3 (Minor Problem)	User can access the Application, and one of the less important functions is not available resulting in a minor impact.
Severity Level 4 (Minor Problem/Enhancement Request)	The impact is insignificant to users, and the Parties agree that problem resolution will require new functionality or an enhancement to be made at a mutually agreed upon date.

Data Integration

Data Integration refers to the receipt, analysis, loading and processing of the law enforcement data. As this data becomes available to Seisint for inclusion in FACTS, Seisint shall process the data and incorporate it in the production application in a timely manner. In no case shall the initial data integration of a law enforcement data file exceed sixty (60) days following receipt of such file at Seisint's data center.

User Documentation

To assist the users in their daily application use, a number of documents have been created and distributed to the users.

- FACTS Application User Guide – this document outlines the features and capabilities of the system and how they function.
- Training Exercises – this document provides 14 guided exercises to illustrate the power of the system and each capability.
- Technical Support / Troubleshooting Guide – this document provides a troubleshooting guide and useful phone numbers to call in the event of login/access problems, application usage questions, or installation problems.

Training

Seisint and the Florida Department of Law Enforcement have teamed up to create a training program for FACTS. At this time the training program includes a "Train the Trainer" class, where approved users get hands-on training at their site by FACTS trainers. It is intended that this group of trainees will be able to train additional state approved users following the completion of the course.

FACTS™ Application Train the Trainer Course Description
Duration: 1 day
Student Prerequisites: User Security Agreement signed
State/Agency Prerequisites: Legal responsibilities complete, completion of the connection and install test, Agency Security Agreement signed
Maximum class size: 15 people

Summary:

The Train the Trainers class provides an introduction to the FACTS™ Application to approved users. The course can be provided at the location where analysts will use the application on a daily basis. It is intended to familiarize the students with the available application functions and capabilities and prepare them to train additional users in their state.

The class is interactive and hands-on, and includes a detailed product demonstration and tutorial on proper application use. The following topics are included in the class:

- Introduction
- Permissible Application Uses
- Available data sources
- Detailed instructions on the following functions:
  - Person Search
  - Driver's License Search
  - Motor Vehicle Search
  - Phone Lookup
  - Company Search
  - Department of Corrections Search
  - Criminal History Search
  - Lineup
  - Montage
  - Wildcard Search
  - Criminal Data Analysis
  - SocialNet
  - Mapping
- Helpful Investigation Tips
- Self-guided exercises and practice cases
- Question and Answer period

FACTS Licensing and Support Fees

Seisint is pleased to be selected to support the MATRIX Pilot Program. We appreciate the opportunity to again serve the law enforcement community. We understand the pilot is scheduled to begin on November 1, 2003 and end on October 31, 2004.

Seisint is prepared to provide access to FACTS for all 13 participating states. We will issue up to 3,050 FACTS user licenses, which expire on October 31, 2004. Under this license model, the MATRIX Board has the flexibility to allocate FACTS licenses to law enforcement agencies in the pilot states in any manner of their choosing. Pilot states desiring to expand their user access above the allocated licenses can purchase additional licenses at a rate of $133 per user per month.

FACTS™ Funding Schedule	
3,050 FACTS User Licenses (Expiring October 31, 2004)	$4,867,800
Supercomputing and Network Hardware Platform Data Center Space, Security, and Operations Staff Ongoing Data Integration Services 24 X 7 Customer Support and Service Help Desk 26 User Training Session (including travel expenses) Continued Application Enhancements	$2,932,200
TOTAL	$ 7,800,000

FACTS funding is payable in 12 equal payments of $ 650,000 due on the 15th of each month beginning on November 15th, 2003.

Summary

Seisint is proud of our growing relationship with law enforcement. We believe FACTS is a unique investigational product not otherwise available in the marketplace. We were pleased to receive a confirmation of our belief with the sole source award by the U.S. Department of Justice. We are pleased to provide Seisint's FACTS to the Matrix Program to give law enforcement the ability to respond instantly to the challenges they face. We will continue the innovative development relationship started 18 months ago and expand it to include the larger law enforcement community of the participating MATRIX states. The result will be the re-invention of the way law enforcement agencies share information and, therefore, a safer community for our families.

To this goal, we are dedicated.