Y490 Politics of the Internet

November 5, 2009
“...routine ways in which focused attention is paid to personal details by organizations that want to influence, manage, or control certain persons or population groups. It occurs for all kinds of reasons, which can be located on a continuum from care to control. Some element of care and some element of control are nearly always present, making the process inherently ambiguous.”

David Lyon as quoted in Chadwick, p. 258.
Surveillance Theory

- Bentham’s panopticon
- Foucault (study of prisons)
- Rhizomic surveillance
Total/Terrorism Information Awareness Program, 2002

- Program headed by Adm. John Poindexter
  - National Security Advisor to President Reagan
  - Tried and convicted on felony charges for his involvement in the Iran-Contra scandal
  - Conviction was later reversed on appeal
Functions of TIA

- Use data gained from component technologies to create a large-scale national counterterrorism database
- Populate the database, and look for methods for mining, combining and refining new sources to include in the database
- Analyze and correlate information in the database to derive actionable intelligence
Translingual Information Detection, Extraction, and Summarization (TIDES)
Develop advanced language processing technology to enable English speakers to find and interpret critical information in multiple languages without requiring knowledge of those languages.

Wargaming the Asymmetric Environment (WAE)
WAE identifies predictive indicators of attacks by examining terrorist behavior in the broader context of their political, cultural, and ideological environment.

Evidence Extraction and Link Discovery (EELD)
Develop detection capabilities to extract relevant data and relationships about people, organizations, and activities from message traffic and open source data.

Total Information Awareness
- Architectures for a large-scale, counterterrorism database.
- Novel methods for populating the database from existing sources, creating innovative new sources, and inventing new algorithms for mining, combining, and refining information for subsequent inclusion into the database.
- Revolutionary new models, algorithms, methods, tools, and techniques for analyzing and correlating information in the database to derive actionable intelligence.

Genoa & Genoa II
Information technology for the intelligence community to rapidly and systematically accumulate evidence, facilitate collaboration, and test hypothesis that support decision-making. Genoa II will develop and deploy collaborative tools to allow humans and machines to "think together."

Human ID at a Distance
Develop automated biometric identification technologies to detect, recognize, and identify humans at great distances.

Bio-Surveillance
Exploit nontraditional data sources to enable early detection and warning of a bio-terrorist event.

Genisys
Produce technology enabling ultra-large, all-source information repositories.
TIA Programs

- Translingual Information Detection, Extraction and Summarization (TIDES)
  - Translation program (documents, chat rooms, video etc)
- Wargaming the Asymmetric Environment (WAE)
  - “Market betting” on the likelihood of a terror attack based on socio-economic and political events
- Human ID at a Distance
  - Improved facial recognition technology, gait recognition, physique recognition (height, estimated weight etc...)
- BIO Surveillance
  - Early warning of a biological attack (anthrax, smallpox, etc...)
More TIA Programs

- Genysis
  - Large database of public and private data

- Genoa I/II
  - Collaboration tools to enable analysts from different agencies to share information and ideas
    - A classified Wikipedia

- Evidence Extraction and Link Discovery (EELD)
  - Search tool to help the analyst determine “who knows whom” and which organization is involved with what people and activities
    - “Six degrees of Kevin Bacon”
Many of the accounts lead back to one man - Mustafa Ahmed - an elusive character who is emerging as a crucial link between the Saudi exile Osama bin Laden and the perpetrators of the worst act of terrorism on American soil. FBI investigators believe Ahmed was the banker who helped distribute the finances for the operation, which is now believed to have cost $US200,000,000 ($406,000).

The suspected hijackers' ringleader, Egyptian Mohamed Atta, wired $US10,000 to two Middle Eastern accounts a few days before the attacks. More money was funnelled back by Nabil al Marabih, regarded as a key link in a Boston cell loyal to bin Laden which appears to have figured prominently in arranging accommodation and transport in the final days before the attack.
Total Information Awareness of transnational threats requires keeping track of individuals and understanding how they fit into models.
Civil Libertarian Objections

- Based on the COINTELPRO (COunterINTELligencePROgram) of the 1960’s
  - FBI abuse of the privacy rights of anti-war and civil rights activists in the 1960s under the blanket justification of national security
- Main objection is the protection of private data and privacy issues
  - TIA essentially a data-mining program
    - Would sift through massive amounts of private data in order to “sniff” out terrorist activity
    - No guarantees of citizens’ protection from abuse of this data
## Definition of Data Mining

<table>
<thead>
<tr>
<th>Evolutionary Step</th>
<th>Enabling Technologies</th>
<th>Product Providers</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection (1960s)</td>
<td>Computers, tapes, disks</td>
<td>IBM, CDC</td>
<td>Retrospective, static data delivery</td>
</tr>
<tr>
<td>Data Access (1980s)</td>
<td>Relational databases (RDBMS), Structured Query Language (SQL), ODBC</td>
<td>Oracle, Sybase, Informix, IBM, Microsoft</td>
<td>Retrospective, dynamic data delivery at record level</td>
</tr>
<tr>
<td>Data Warehousing &amp; Decision Support (1990s)</td>
<td>On-line analytic processing (OLAP), multidimensional databases, data warehouses</td>
<td>Pilot, Comshare, Arbor, Cognos, Microstrategy</td>
<td>Retrospective, dynamic data delivery at multiple levels</td>
</tr>
<tr>
<td>Data Mining (2000s)</td>
<td>Advanced algorithms, multiprocessor computers, massive databases</td>
<td>Pilot, Lockheed, IBM, SGI, numerous startups (nascent industry)</td>
<td>Prospective, proactive information delivery</td>
</tr>
</tbody>
</table>
Datamining: False Negatives

An analyst runs a search for recent foreign travel and purchase of chemicals used in explosives and gets a result in which a single credit card number purchased a ticket from Tel Aviv, Israel to St. Louis, Missouri, and the purchase of a large amount of fertilizer a short time afterwards. Does this result indicate:

- A.) A terrorist infiltrating the U.S. to place a truck bomb at the Golden Arch?
- B.) An American farmer returning from a trip to the Holy Land?
ACLU: Questions raised about TIA

- Would TIA be limited to an arbitrary number of databases, or is the number of databases unlimited?
- What kinds of analysis would TIA be capable of?
  - Would it be limited strictly to terrorism or could any type of search be possible? (ex. Anti-war groups, drug use, jaywalking)
- What difference does a distributed database make?
  - DARPA officials state that TIA would not be a centralized database, the ACLU stated that this did not matter
- How will TIA affect the American legal tradition of individual suspicion?
DARPA’s Views on Legal Issues Surrounding TIA

• Insisted that TIA was not a domestic surveillance program
  • Intended focus on foreign activity
• TIA would have had a built-in audit control system to identify abusers of the system
• While DARPA acknowledged the TIA could outpace existing privacy protections, TIA was very early in development and was using only data legally usable or synthetically generated
  • Privacy protections had time to “catch up” to TIA
What Killed TIA?

- No guarantees that TIA would not be used for domestic surveillance
  - FBI collaboration on the project indicated a domestic aspect of TIA
- Privacy protections were not originally conceptualized with the program
  - Added after controversy over the program erupted
- No defined limits to databases TIA would access
- Choice of Poindexter to head program
## List of Federal Government Counterterrorist Data Collection and Mining Programs

<table>
<thead>
<tr>
<th>Name</th>
<th>Administered by</th>
<th>Period of Operation</th>
<th>Scope of Operation</th>
<th>Types of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able Danger</td>
<td>Defense, SOCOM</td>
<td>1999-2000</td>
<td>Al Qaeda and Bosnia</td>
<td>Classified and commercial</td>
</tr>
<tr>
<td>TIA</td>
<td>Defense, DARPA</td>
<td>2002-2004</td>
<td>Research on new counterterrorism data mining techniques</td>
<td>Classified and commercial</td>
</tr>
<tr>
<td>CAPPS II</td>
<td>Homeland Security</td>
<td>2001-2004</td>
<td>Preventing hijacking and airline-based terrorism</td>
<td>Airline passenger personal information</td>
</tr>
<tr>
<td>MATRIX</td>
<td>Consortium of States</td>
<td>2001-2005</td>
<td>Targeting of potential criminals and terrorists</td>
<td>State public records and law enforcement data</td>
</tr>
<tr>
<td>SEVIS</td>
<td>Homeland Security</td>
<td>2001-present</td>
<td>Detecting terrorists in colleges, universities, and schools</td>
<td>Data on exchange students and foreign visitors</td>
</tr>
<tr>
<td>ATS</td>
<td>Homeland Security</td>
<td>Late 1990s to present,</td>
<td>Preventing terrorists and terrorist weapons from entering the</td>
<td>Passenger and cargo data, especially, but also other data</td>
</tr>
<tr>
<td>US-VISIT</td>
<td>Homeland Security</td>
<td>2004-present</td>
<td>Tracking entrants to US</td>
<td>Photograph and finger-print data</td>
</tr>
<tr>
<td>Project Strikeback</td>
<td>FBI, Education</td>
<td>2001-2006</td>
<td>Tracking college aid money to potential terrorists</td>
<td>Financial aid records of individuals</td>
</tr>
</tbody>
</table>
Reason for Cancellation of Data Mining Programs

- Inability of the programs to meet their technical goals because of poor data, faulty algorithms, interoperability problems, and the generation of too many “false positives”
- Inability of the programs to adequately address privacy concerns
- The non-transparent combination of classified and open-source data in some programs
- The general lack of transparency in most of the programs
- The potential for other forms of abuse besides privacy violations, or “mission creep” (the use of data for purposes other than those originally stated).
Legal Environment for Warrantless Wiretaps

- 1978 **Foreign Intelligence Surveillance Act** (FISA)
- 1994 **Communications Assistance for Law Enforcement Act** (CALEA)
- 2003 **Domestic Security Enhancement Act** (Patriot Act)
- March 2004 – Cheney, Gonzalez, and Card visit Attorney General John Ashcroft in the hospital to authorize warrantless wiretaps
- 2006 story about **NSA phone call database**
Protect America Act of 2007

- Amended FISA to remove requirement for warrants
- Made the Attorney General and the Director of National Intelligence responsible for authorizing warrantless searches
- Reauthorized aspects of the Patriot Act that were expiring
FISA Amendments Act of 2008

- Reauthorizes FISA, expands Presidential powers to authorize warrantless searches
- Gives telecommunications firms immunity for past cooperation with federal intelligence and law enforcement agencies
- Rachel Maddow video