Countering Terrorism through Information and Privacy Protection Technologies

Robert Popp, John Poindexter

IEEE Security & Privacy, vol. 4, no. 6, Nov.-Dec. 2006

Terrorism

Terrorists

- highly adaptive, secretive networks
- indistinguishable from normal population
- use public infrastructure
- ruthless (kill civilians, employ WMD, . . .)

Terrorism

Terrorists

- highly adaptive, secretive networks
- indistinguishable from normal population
- use public infrastructure
- ruthless (kill civilians, employ WMD, . . .)

Counterterrorism

objective	detect and identify terrorists
assumption	planning involves people, which leave traces
approach	pattern-based analysis of distributed data
problems	models, noise/amount of data, civil liberties

Information Technology

(Collection and) Analysis of Data

- modeling tools
- cooperation
- (graphical) presentation
- natural language and multimedia processing
- data mining

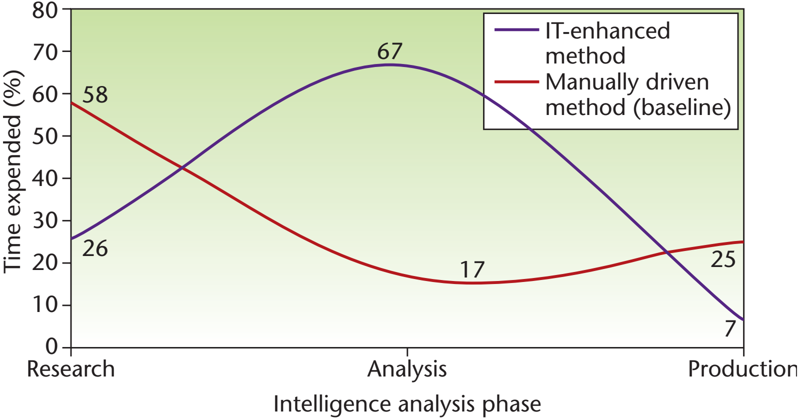
Information Technology

(Collection and) Analysis of Data

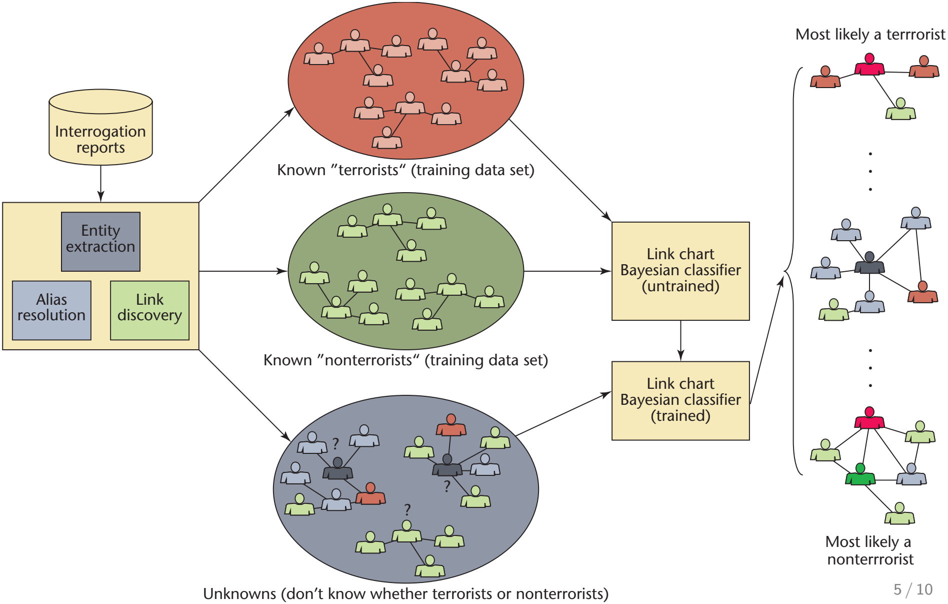
- modeling tools
- cooperation
- (graphical) presentation
- natural language and multimedia processing
- ~~data mining~~ data analysis/terrorism detection

Data Mining	vs.	Terrorism Detection
Discover models/patterns		Detect (rare) patterns
Independent instances		Networks
Sampling okay		Sampling destroys connections
Homogenous data		Heterogenous data

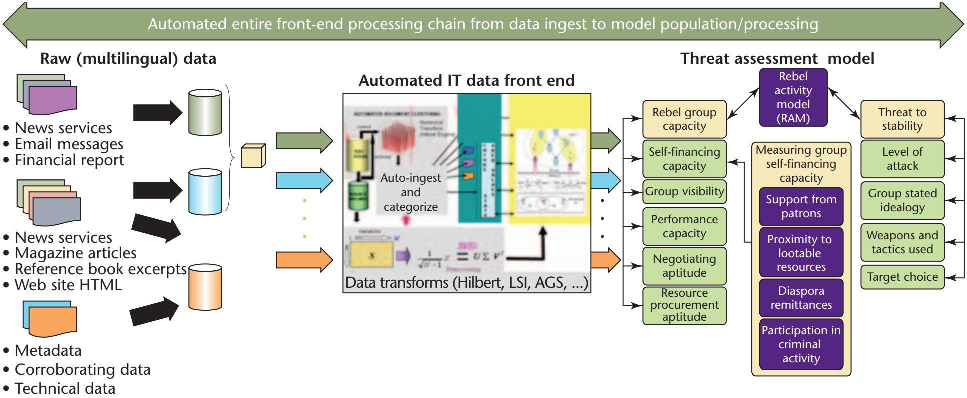
Example 1 – Al Qaeda’s WMD Capabilities



Example 2 – Guantanamo Inmates


Interrogation reports
Entity extraction
Alias resolution
Link discovery
Known ”terrorists“ (training data set)
Known ”nonterrorists“ (training data set)
Unknowns (don’t know whether terrorists or nonterrorists)
?
?
?
Link chart Bayesian classifier (untrained)
Link chart Bayesian classifier (trained)
Most likely a terrrorist
Most likely a nonterrrorist

Example 3 – Instability of National States



Automated entire front-end processing chain from data ingest to model population/processing

Raw (multilingual) data

- News services
- Email messages
- Financial report

- News services
- Magazine articles
- Reference book excerpts
- Web site HTML

- Metadata
- Corroborating data
- Technical data

Automated IT data front end

Auto-ingest and categorize

Data transforms (Hilbert, LSI, AGS, ...)

Threat assessment model

Rebel group capacity

Self-financing capacity

Group visibility

Performance capacity

Negotiating aptitude

Resource procurement aptitude

Rebel activity model (RAM)

Measuring group self-financing capacity

Support from patrons

Proximity to lootable resources

Diaspora remittances

Participation in criminal activity

Threat to stability

Level of attack

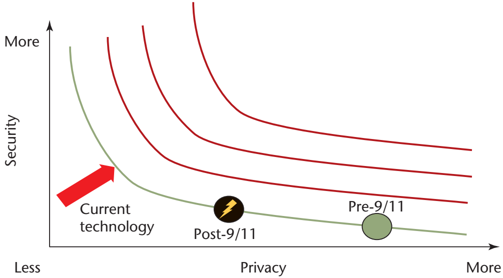
Group stated idealogy

Weapons and tactics used

Target choice

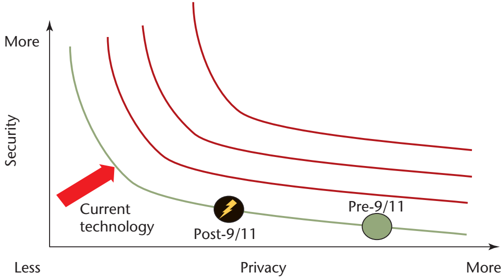
Privacy

[...] our goal (and challenge) is to maximize security at an acceptable level of privacy.



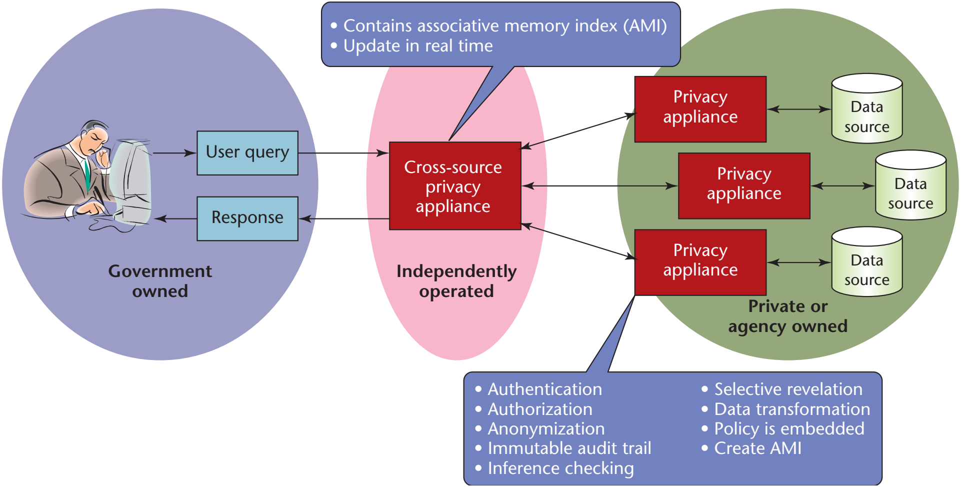
Privacy

> *[...] our goal (and challenge) is to maximize security at an acceptable level of privacy.*



> *[...] for a working definition, we would argue that personal privacy is only violated if the violated party suffers some tangible loss, such as unwarranted arrest or detention, for example.*

Privacy Appliance Concept



- Contains associative memory index (AMI)
- Update in real time

User query

Response

Cross-source privacy appliance

Privacy appliance

Privacy appliance

Privacy appliance

Data source

Data source

Data source

Government owned

Independently operated

Private or agency owned

- Authentication
- Authorization
- Anonymization
- Immutable audit trail
- Inference checking
- Selective revelation
- Data transformation
- Policy is embedded
- Create AMI

Privacy Technologies

Data Transformation blinding

Anonymization pseudonymization

`[name (first, last), telephone (area code, exchange, line number), address (street, town, state, zip code)]`

$$\Downarrow$$

`[name (first), telephone (area code), address (state),` *ID*`]`

Privacy Technologies

Data Transformation blinding

Anonymization pseudonymization

`[name (first, last), telephone (area code, exchange, line number), address (street, town, state, zip code)]`

⇓

`[name (first), telephone (area code), address (state),` *ID*`]`

Selective Revelation incremental access to data

Immutable Audit audit logs kept by *trusted 3rd party*

Self-reporting Data central authority for “truth maintenance”

Privacy Policies

Neutrality existing laws apply to new technology

Minimize Intrusiveness anonymize/pseudonymize personal data

Intermediate Not Ultimate Consequence analysts as safeguard

Audits And Oversight built-in technological safeguards

Accountability of the executive to the legislative

Necessity of redress mechanisms for false positives

People and policy oversight and penalties for abuse