

Security Analytics on Online Social Networks: Identifying Insiders and Raising Community Awareness

Miltos Kandias, Vasilis Stavrou

October 2014

Technical Report AUEB/INFOSEC/Rev-1014/v.1.1
INFOSEC Laboratory, Dept. of Informatics
Athens University of Economics & Business
October 2014

Security Analytics on Online Social Networks: Identifying Insiders and Raising Community Awareness

Miltos Kandias, Vasilis Stavrou

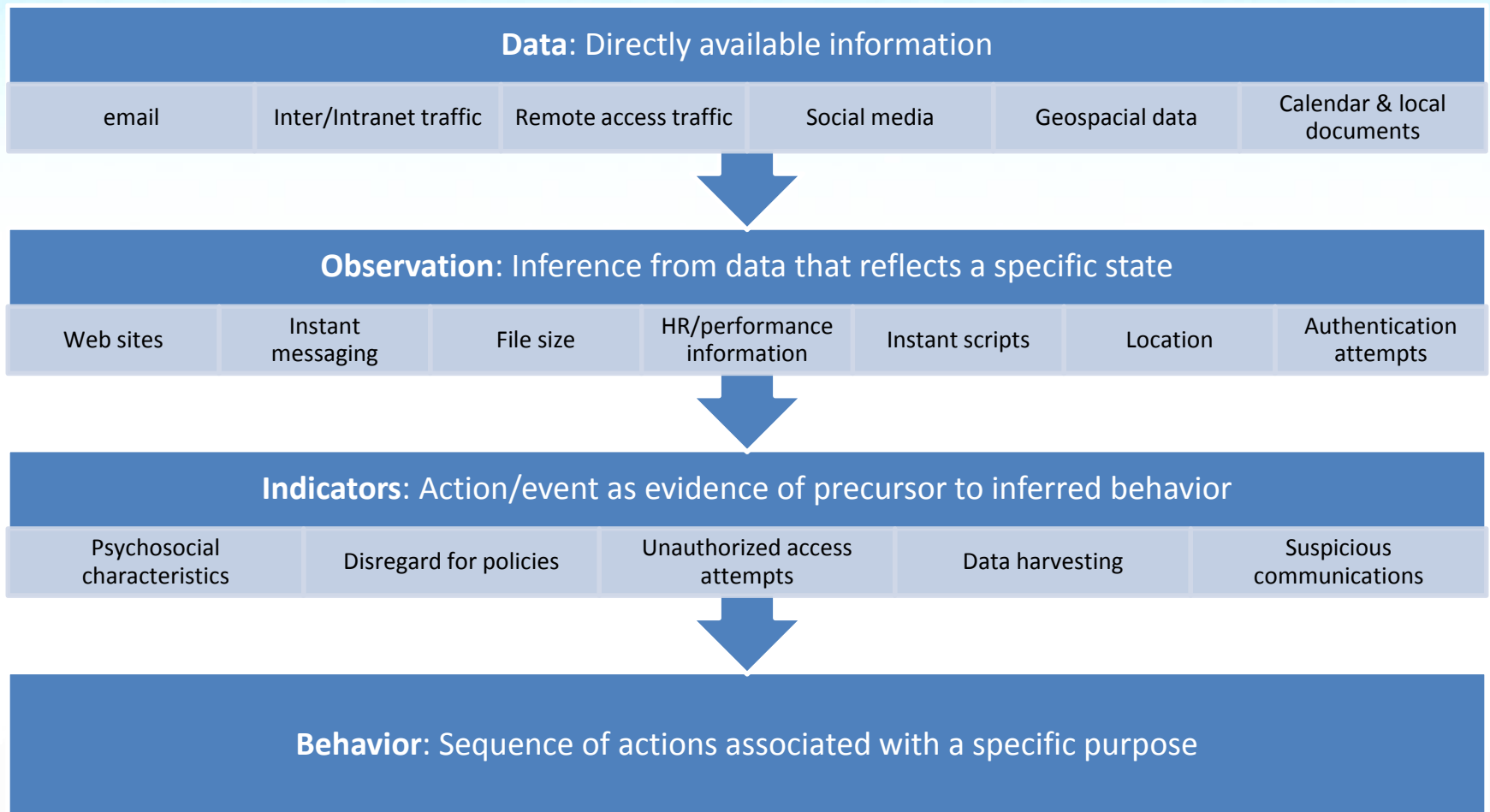
Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business, Greece



Outline

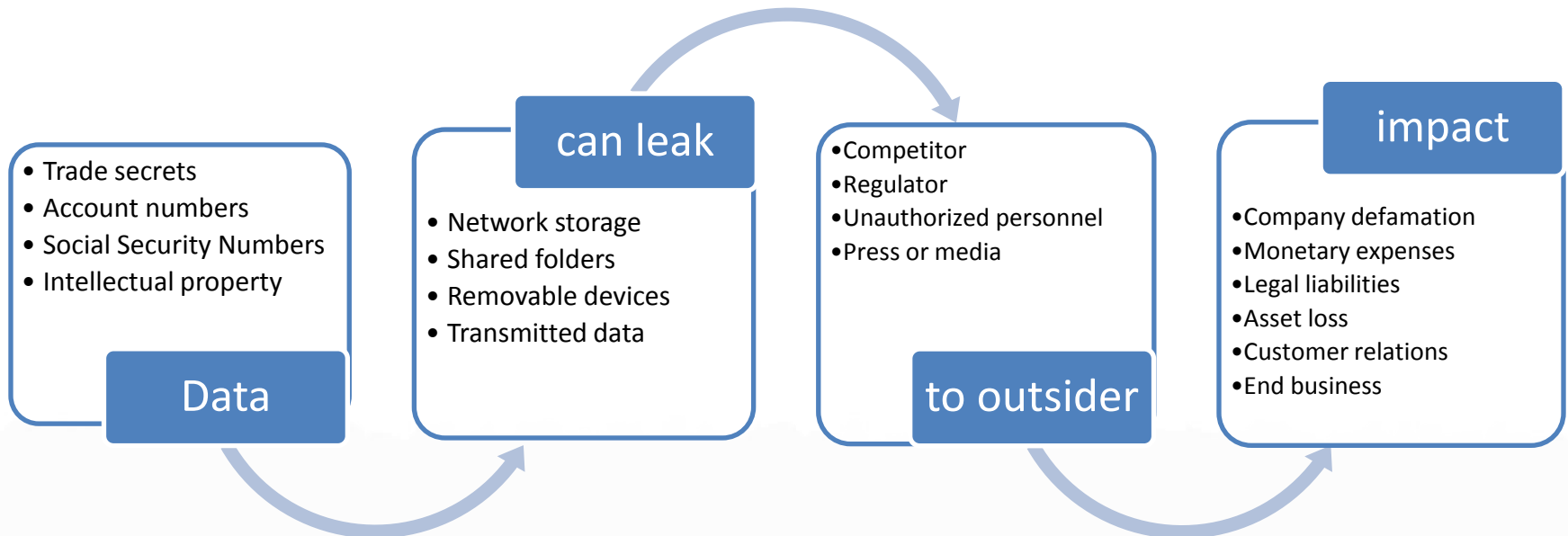
- Online Social Networks (OSN)
- Security Analytics & Open Source Intelligence (OSINT)
- The insider threat
- Behavior prediction capabilities
 - Case 1:** Success story - Insider detection and narcissism
 - Case 2:** Success story - Predicting delinquent behavior
 - Case 3:** Success story - Detecting stress levels
 - Case 4:** Horror story - Revealing political beliefs
- Ethical and legal issues
- Conclusions

A generic model for predicting threats



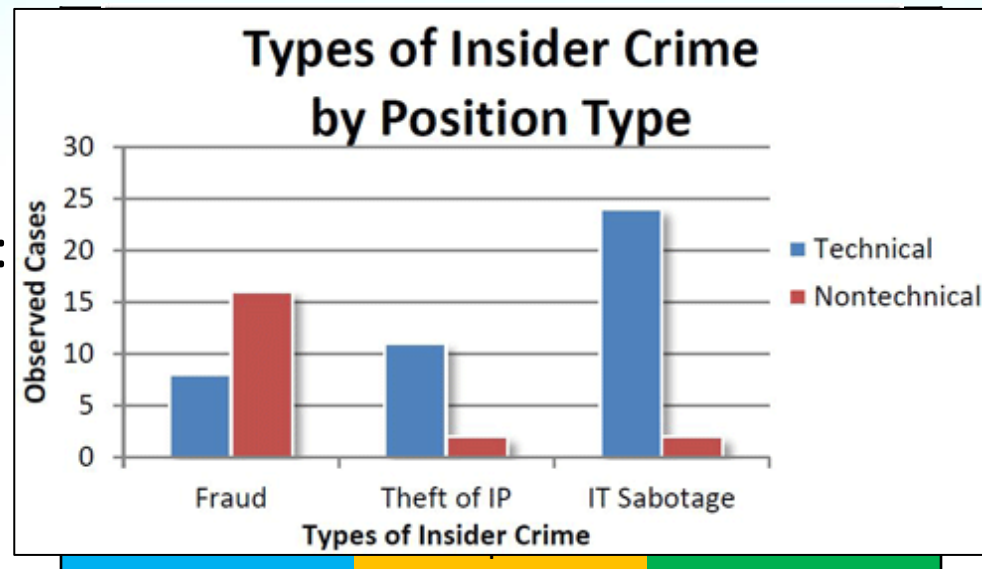
Insider Threat

- The insider threat is a severe problem in cyber/corporate security, which originates from persons who:
 - are legitimately given access rights to information systems,
 - misuse privileges and
 - violate security policy.



Insider Threat Impact & Severity

- Taxonomy of insider threat impact.
- Insider threat the most important security issue for 2014 (top priority to protect):
 - Case of US Government contractor E. Snowden casting shadow over 2014.
- Insiders consist the top source of data breaches.
- Insider crime indicative categories.



Source: Gartner Group, Report 5605
2011 Cyber Security Watch Survey: How Bad Is the Threat? CERT
<http://www.scribd.com/doc/101111111/Top-10-Issues-in-IT-Security-for-2014/>
Carnegie Mellon University, USA
ZDNet Asia IT Priorities Survey 2008/09

The threat

- **Motive**
- Opportunity
- Vulnerability
- Skills

- Opportunity
- **Motive**
- **Ability to overcome inhibitions**
- Stimulus/impulse

Threat consists of:

Malevolent user requirements:

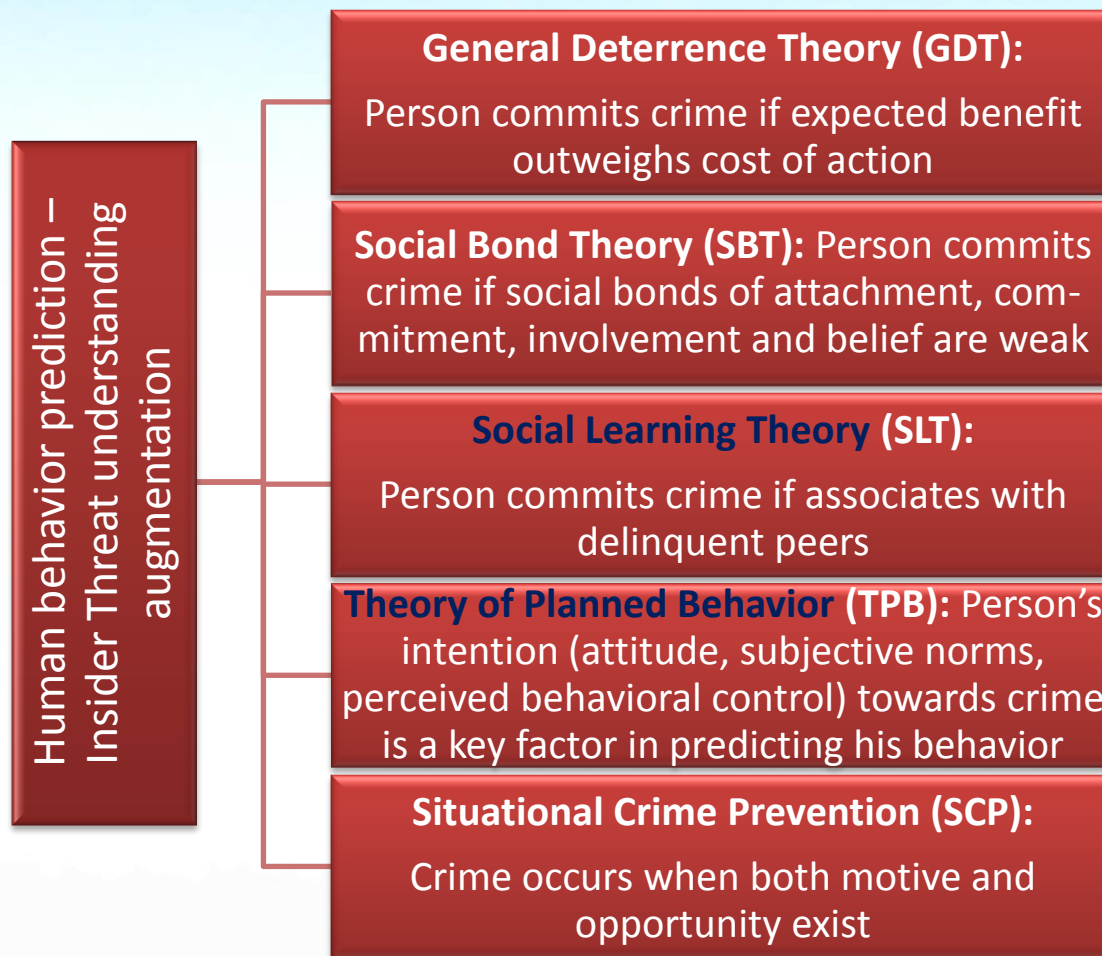
- **Introversion**
- **Social and personal frustrations**
- Computer dependency
- Ethical "flexibility"
- **Reduced loyalty**
- **Entitlement-Narcissism**
- Lack of empathy
- **Predisposition towards law enforcement**

Personal factors (Shaw)

Personal factors (FBI)


- Greed/financial need
- **Anger/Revenge**
- **Problems at work**
- **Ideology/Identification**
- **Divided loyalty**
- Adventure/Thrill
- Vulnerability to blackmail
- **Ego/self-image (Narcissism)**
- Ingratiation
- Compulsive and destructive behavior
- Family problems

Delinquent behavior prediction theories



Case 1

Scope: Insider threat prediction based on Narcissism

OSINT		OSN: Twitter 
Tools used for the analysis		
Science	Theory	
Computing	Graph Theory	
Sociology	Theory of Planned Behavior	
	Social Learning Theory	

Case 1: Insider threat prediction based on Narcissism



Narcissistic behavior detection

Study: Motive, ego/self-image, entitlement

Means: Usage Intensity, Influence valuation, Klout score

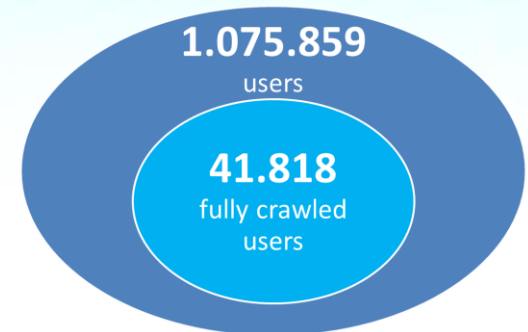
- Individuals tend to transfer offline behavior online.
- Convicted insiders do share this personality trait (narcissism).
- Utilize graph theoretic tools to perform analysis.
- Detection via social media popularity and usage intensity.
- Trait of narcissism relates to delinquent behavior via :
 - sense of entitlement,
 - lack of empathy,
 - anger and “revenge” syndrome and
 - inflated self-image.



Dataset: General parameters

- Focus on a Greek **Twitter** community:
 - Context sensitive research.
 - Utilize ethnological features rooted in locality.
 - Extract and analyze results.
- Analysis of **content** and measures of **user influence** and **usage intensity**.
- User categories: follower, following and retweeter.
- Graph:
 - Each user is a node.
 - Every interaction is a directed edge.
- **41.818** fully crawled users (personal and statistical data)
 - Name, ID, personal description, URL, language, geolocation, profile state, lists, # of following/followers, tweets, # of favorites, # of mentions, # of retweets.

Twitter (Greece, 2012-13)



7.125.561 connections
among them

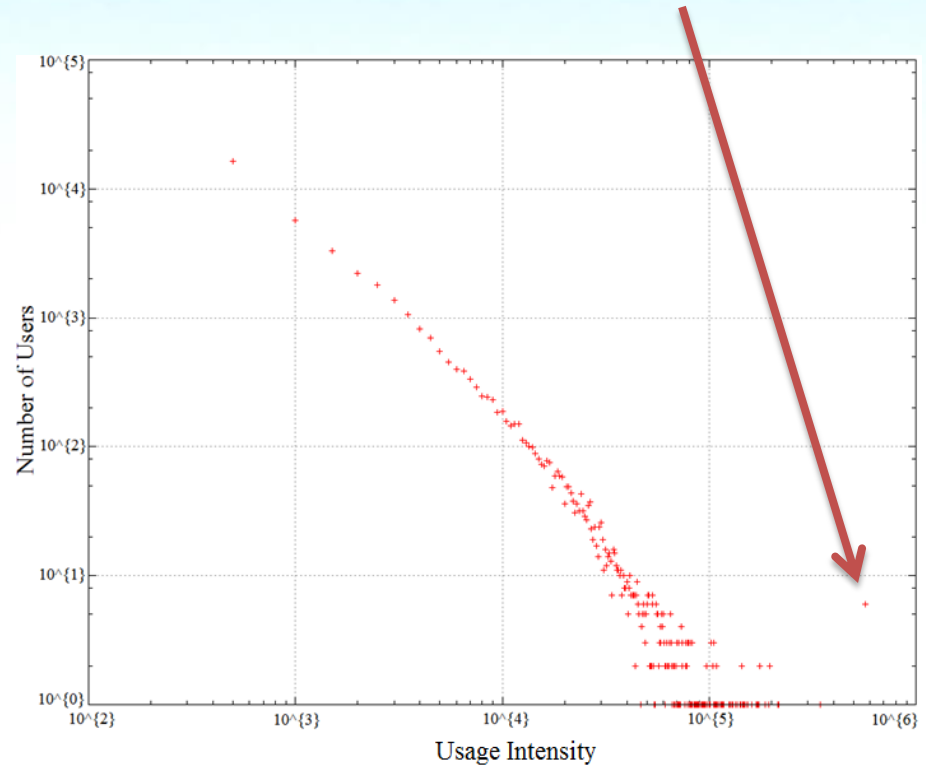
Graph Theoretical approach



- **Strongly connected components:**
 - There exists 1 large component (153.121 nodes connected to each other) and several smaller ones
- **Node Loneliness:**
 - 99% of users connected to someone
- **Small World Phenomenon:**
 - Every user lies <6 hops away from anyone
- **Indegree Distribution:**
 - # of users following each user
 - Average 13.2 followers/user
- **Outdegree Distribution:**
 - # of users each user follows
 - Average 11 followers/user
- **Usage Intensity Distribution:**

Weighted aggregation of {# of followers, #of followings, tweets, retweets, mentions, favorites, lists}

Important cluster of users



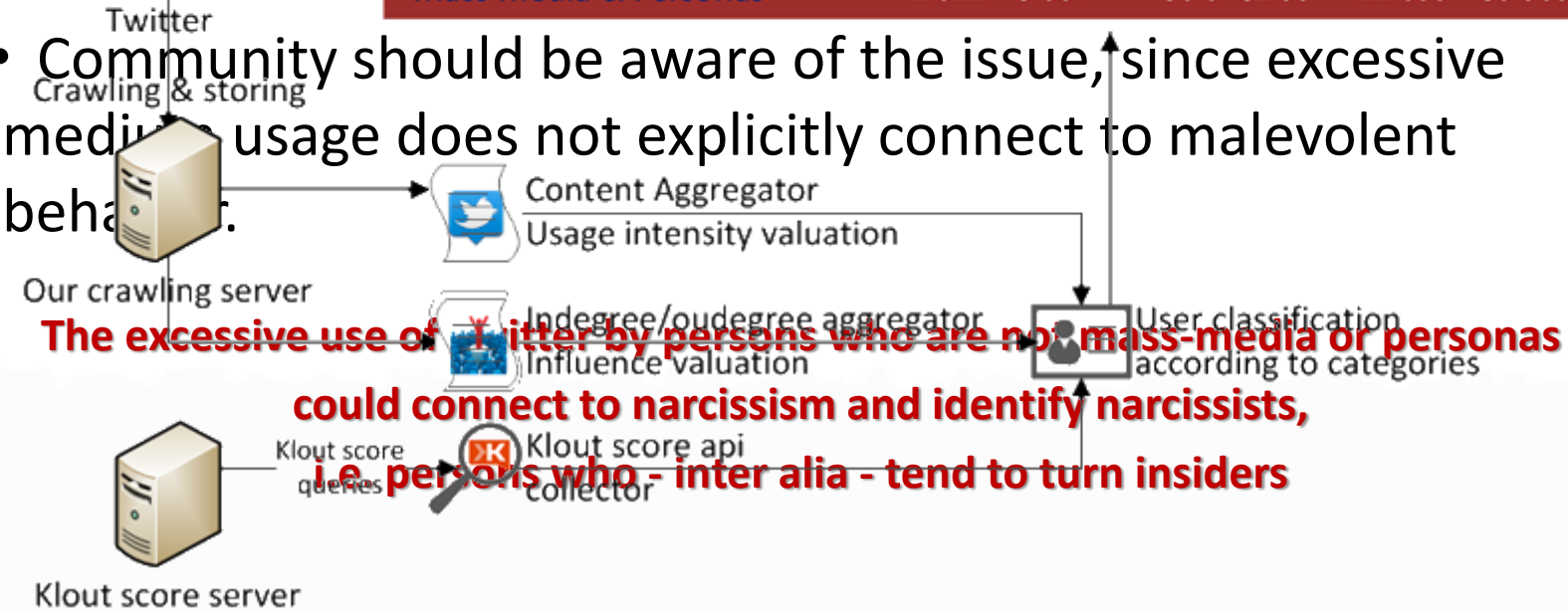


Narcissism detection

- Majority of users make limited use of Twitter.
 - All are “normally” active users and very few “popular” users.
 - Users classified into 4 categories, on the basis of specific metrics (influence valuation, Klout score, usage valuation)


Category	Influence valuation	Klout score	Usage valuation
Loners	0 - 90	3.55 - 11.07	0 - 500
Individuals	90 - 283	11.07 - 26.0	500 - 4.500
Known users	283 - 1.011	26.0 - 50.0	4.500 - 21.000
Mass Media & Personas	1.011 - 3.604	50.0 - 81.99	21.000 - 56.9000

- Above a threshold of activity
 - User becomes “popular”
 - User get a “mass media” status
- Community should be aware of the issue, since excessive media usage does not explicitly connect to malevolent behavior.



Case 2

Scope: Revealing negative attitude towards law enforcement

OSINT		OSN: YouTube 	
Tools used for the analysis			
Science		Theory	
Computing		Machine Learning	
		Data Mining	
Sociology		Social Learning Theory	

Case 2: Revealing negative attitude towards law enforcement



Law enforcement predisposition

Study: Motive, anger, frustrations, predisposition towards law enforcement

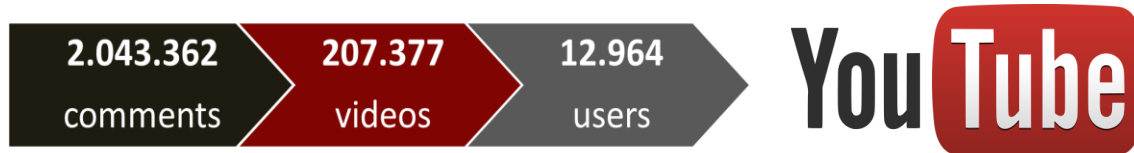
Means: Machine Learning, comment classification, flat data classification.

- Individuals tend to transfer offline behavior online.
- Extract results about users' negative attitude towards law enforcement and authorities.
- Trait of negative attitude towards law enforcement is connected to delinquent behavior via:
 - sense of entitlement,
 - lack of empathy,
 - **anger and revenge syndrome** and
 - inflated self-image.

Dataset: General parameters



- Crawled YouTube and created dataset consists solely of **Greek** users.
- Utilized YouTube **REST-based API** (developers.google.com/youtube/):
 - Only publicly available data collected.
 - Quote limitations (posed by YouTube) were respected.
- Collected data were classified into three categories:
 - user-related information (profile, uploaded videos, subscriptions, favorite videos, playlists),
 - video-related information (license, # of likes, # of dislikes, category, tags) and
 - comment-related information (comment content, # of likes, # of dislikes).

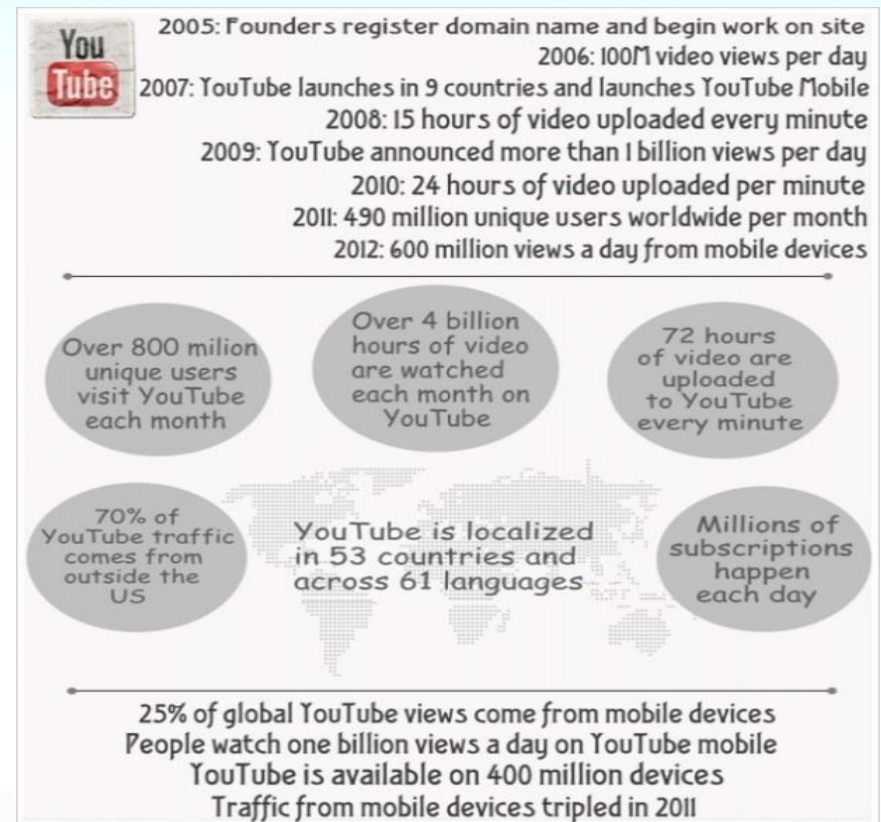


- Time span of collected data covered 7 years (Nov 2005 - Oct 2012).
- A basic anonymization layer added to the collected data:
 - MD5 hashes instead of usernames.

Graph Theory and Content Analysis



- **Small World Phenomenon:**
 - Every user of the community is 6 hops away from everyone else.
- **Indegree Distribution:**
 - Presentation of statistical distribution of incoming edges per node.
- **Outdegree Distribution:**
 - Presentation of statistical distribution of outgoing edges per node.
- **Tag Cloud :**
 - Axis of content of the collected data via tag cloud analysis.
- **YouTube's nature:**
 - Popular social medium, emotional-driven responses, audio-visual stimuli, alleged anonymity, users interact with each other, contains political content.



How was the analysis performed?

We assessed
classifying Y

- Machine Learning
 - Examined
 - Performance
 - Content

Approach	Metrics			
	Machine Learning		Flat Data	
	Classifier	Logistic Regression	Naïve Bayes	
Classes	P	N	P	N
Precision	86	76	72	93
Recall	74	88	92	73
<u>F-Score</u>	80	81	81	82
Accuracy	81		81	

- Flat Data

- An assumption-free method
- An easy-to-scale method
- Both approaches achieve similar results.
- Flat data behaves slightly more efficiently (better f-score).
- Flat data performs faster.
- Flat data verifies the results obtained by Machine Learning.

Machine Learning (1)

- Comment classified into categories of interest:
 - Process performed as **text classification**.
 - Machine trained with **text examples** and the **category** each one belongs to.
 - Excessive support by **field expert** (Sociologist).
- Test set used to evaluate efficiency of resulting classifier:
 - Contains pre-labeled data fed to machine, labeled by field expert.
 - Check if initial assigned label is equal to predicted one.
 - Testing set labels assigned by field expert.
- Most comments are written in Greek – greeklish comments exist.
- Training sets (greeklish, greek) were merged - One classifier was trained.
- Two categories of content were defined:
 - Users with a **negative** attitude (**P**re-disposed negatively (P)).
 - Users with a **not negative** attitude (**N**ot-pre-disposed negatively (N)).

Machine Learning (2)

- **Comment** classification using:
 - Naïve Bayes (NB)
 - Support Vector Machines (SVM)
 - Logistic Regression (LR)
- Classifiers **efficiency** comparison:
 - Metrics (on % basis): Precision, Recall, F-Score, Accuracy
- **Logistic Regression** algorithm:
 - LR classifies a comment with **81% accuracy**

Precision: Measures the classifier exactness. Higher and lower precision means less and more false positive classifications, respectively.

Recall: Measures the classifier completeness. Higher and lower recall means less and more false negative classifications, respectively.

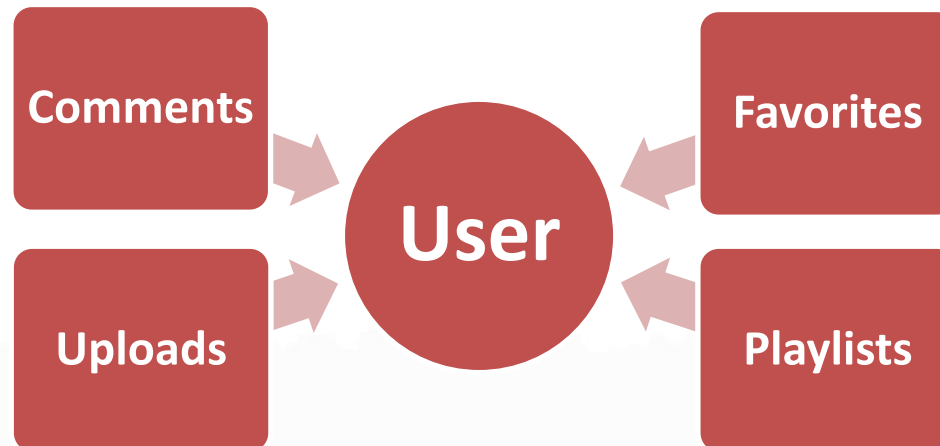
F-Score: Weighted harmonic mean of both metrics.

Accuracy: No. of correct classifications performed by the classifier. Equals to the quotient of good classifications by all data.

Classifier	Metrics					
	NBM		SVM		LR	
Classes	P	N	P	N	P	N
Precision	71	70	83	77	86	76
Recall	72	68	75	82	74	88
<u>F-Score</u>	71	69	79	79.5	80	81
Accuracy	70		80		81	

Machine Learning (3)

- **Video** classification:
 - Examination of a video on the basis of its comments.
 - Voter process to determine category classification.
- **(Video) Lists** classification:
 - Voter process to determine category classification (same threshold).
- Conclusions about **user behavior**:
 - If there is at least one category P attribute then the user is classified into category P.



Example of conclusion extraction

- Each comment falls into a category (P or N) based on the **classifier's prediction**.
- Each video falls into a category based on its **comments**.

Video "Example"			
Comment	Classifier's output	Likes	Dislikes
#1	P	0	2
#2	P	9	1
#3	N	0	5
#4	P	5	2
#5	N	4	13
#6	P	0	3

Only **comments #2 and #4** will be fed to the voter (if N, then ignore. If no likes and at least 1 dislike, then ignore).

Video contains (at least) 2 negatively Predisposed comments. Thus, it falls into category P.

- The voter decides on the basis of the number of P comments (category P).
- Comments with only dislikes and no likes are excluded.
- Same method applies to list of videos (instead of comments), i.e. user's uploaded videos, favourite videos, and playlists.

Flat Data

- Addressing the problem from a different perspective:
 - Connection between users of category P and confidence of accuracy of comments belonging to category P.
 - assumption-free and easy-to-scale method
 - verify (or not) the results of the Machine Learning approach.

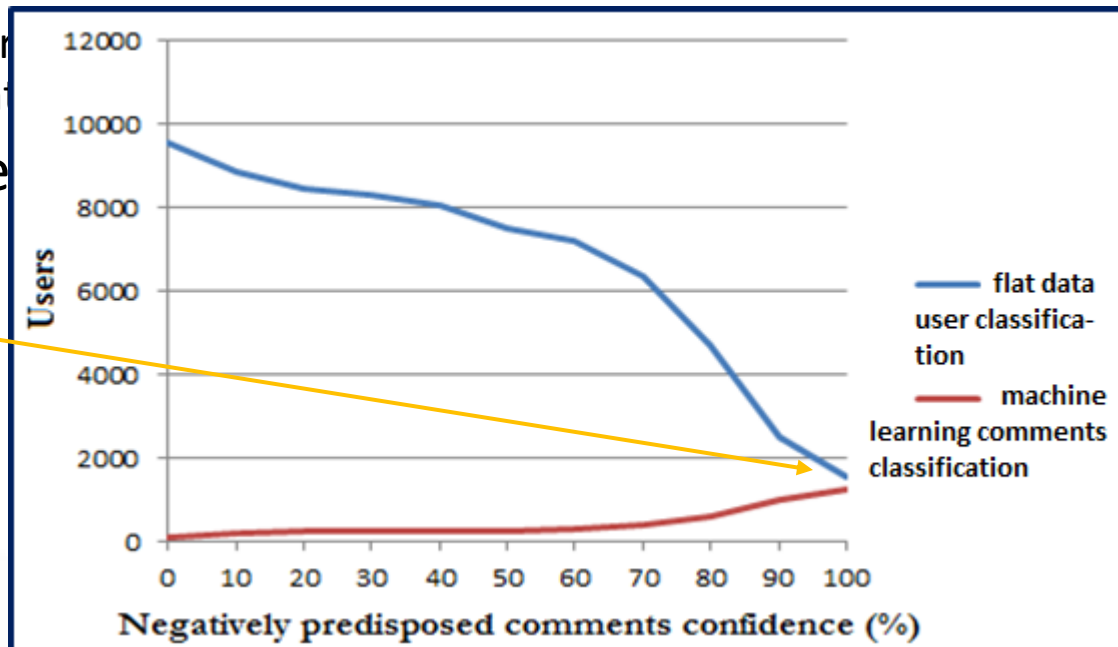
Blue: Users of category P classified on the basis of the comment-oriented tuple (**Flat Data**).

Red: Users of category P classified on the basis of their comments-only (**Machine Learning**).

- Data transformation:

- User repr
- comment

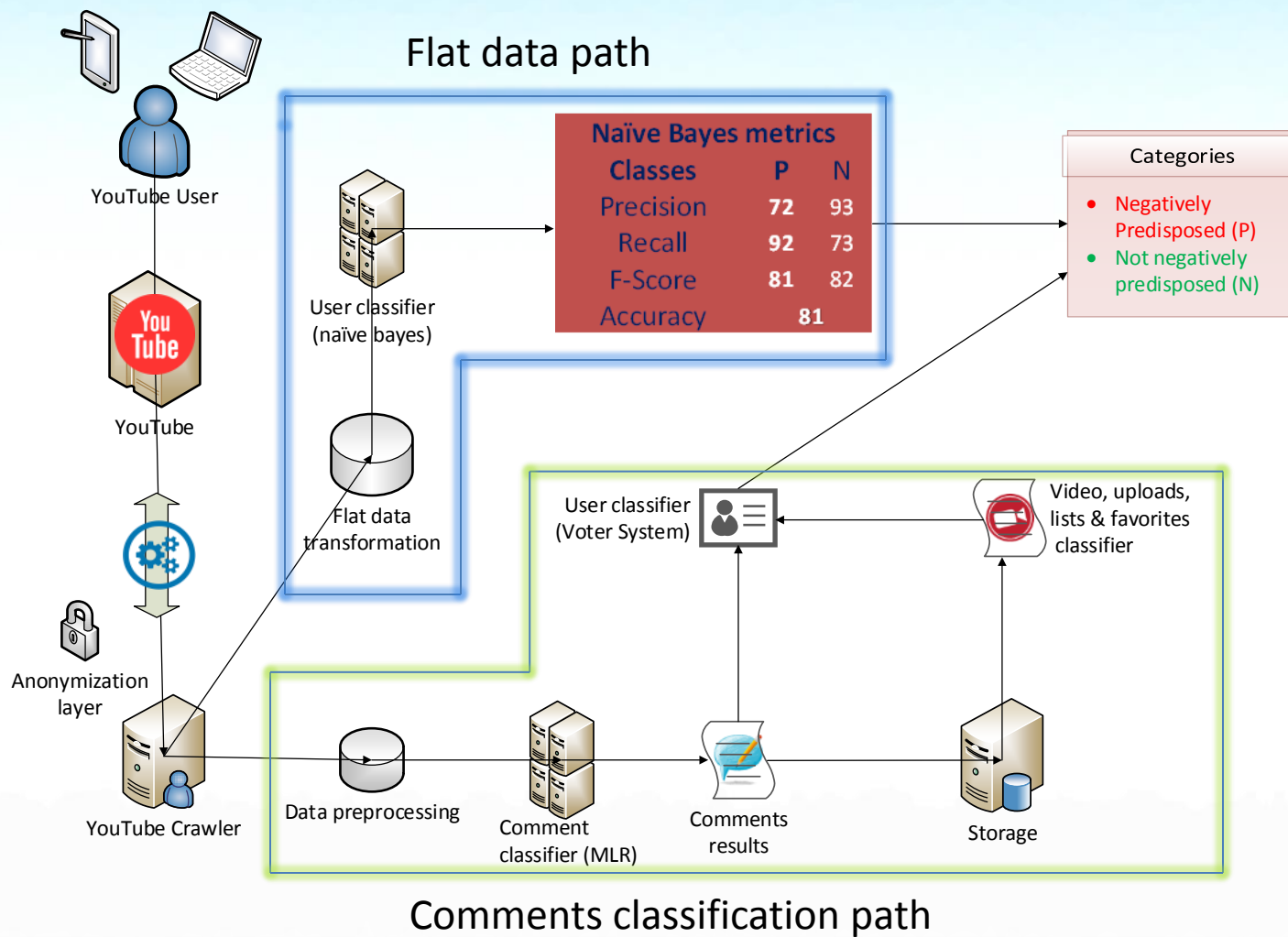
- Machine



1721 users are (almost certainly) negatively predisposed towards law enforcement


to ID the views).
 field expert).

In a nutshell



Case 3

Scope: Detecting stress level usage patterns (overall and over time)

OSINT		OSN: Facebook 	
Tools used for the analysis			
Science		Theory	
Computing		Machine Learning	
		Data Mining	
Sociology		Social Learning Theory	

Case 3: Detecting stress level usage pattern (overall and over time)



Stress level detection

Study: User's overall and over time stress level

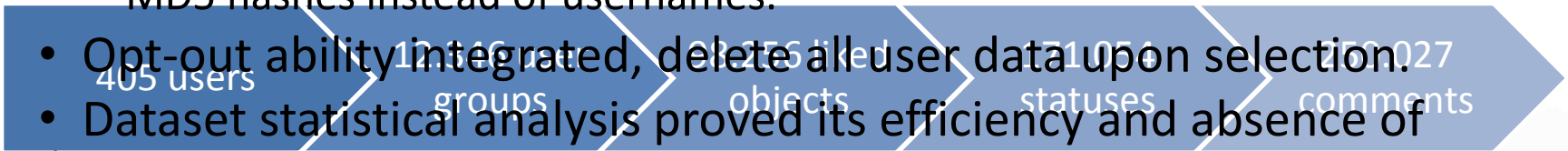
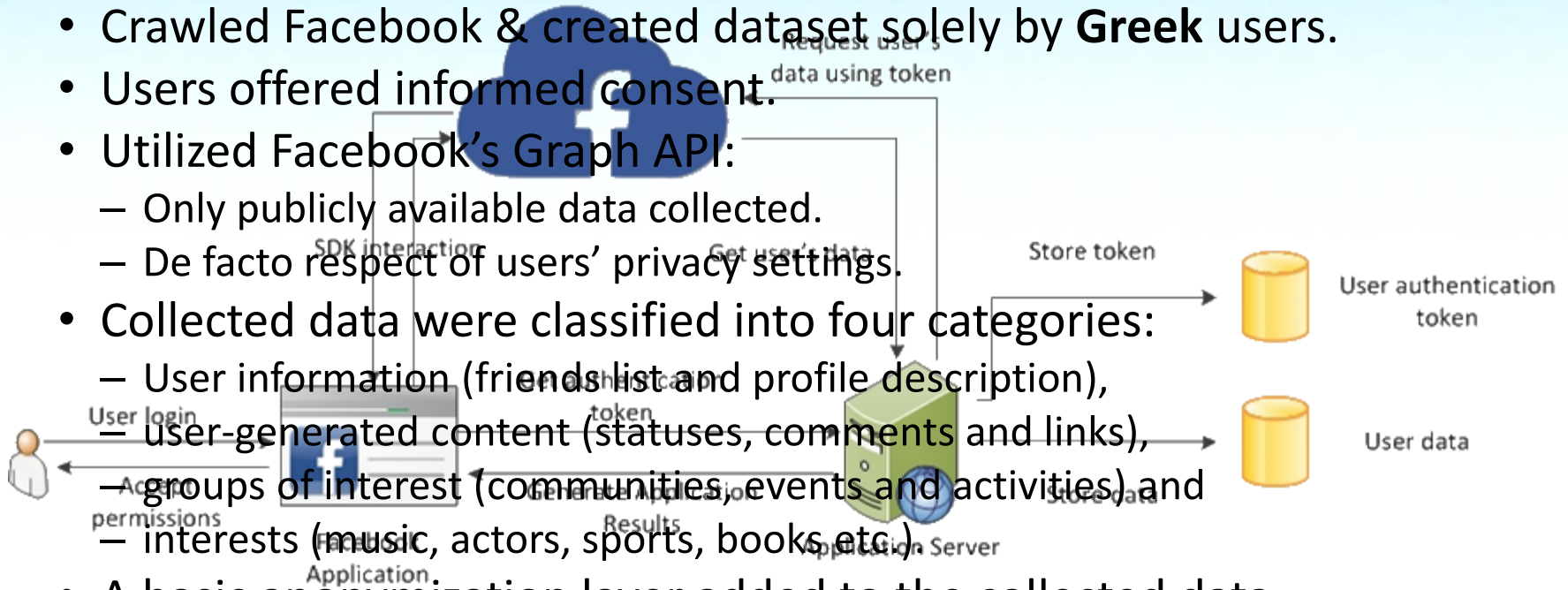
Means: Machine Learning, flat data classification, chronicity analysis.

- Individuals tend to transfer offline behavior online.
- Extract results about usage pattern depicted stress level.
- Analyze each user under the prism of stress level both overall and over time (chronicity analysis).
- High stress has been found to:
 - Make individuals vulnerable to fall prey to third parties.
 - Overcome moral inhibitions.
- Analysis is based on Social Learning Theory and stress correlations are based on Beck's Anxiety Inventory stress test.



Dataset: General parameters

- Crawled Facebook & created dataset solely by **Greek** users.
- Users offered informed consent.
- Utilized Facebook's Graph API:
 - Only publicly available data collected.
 - De facto respect of users' privacy settings.
- Collected data were classified into four categories:
 - User information (friends list and profile description),
 - user-generated content (statuses, comments and links),
 - groups of interest (communities, events and activities) and
 - interests (music, actors, sports, books etc.)
- A basic anonymization layer added to the collected data:
 - MD5 hashes instead of usernames.

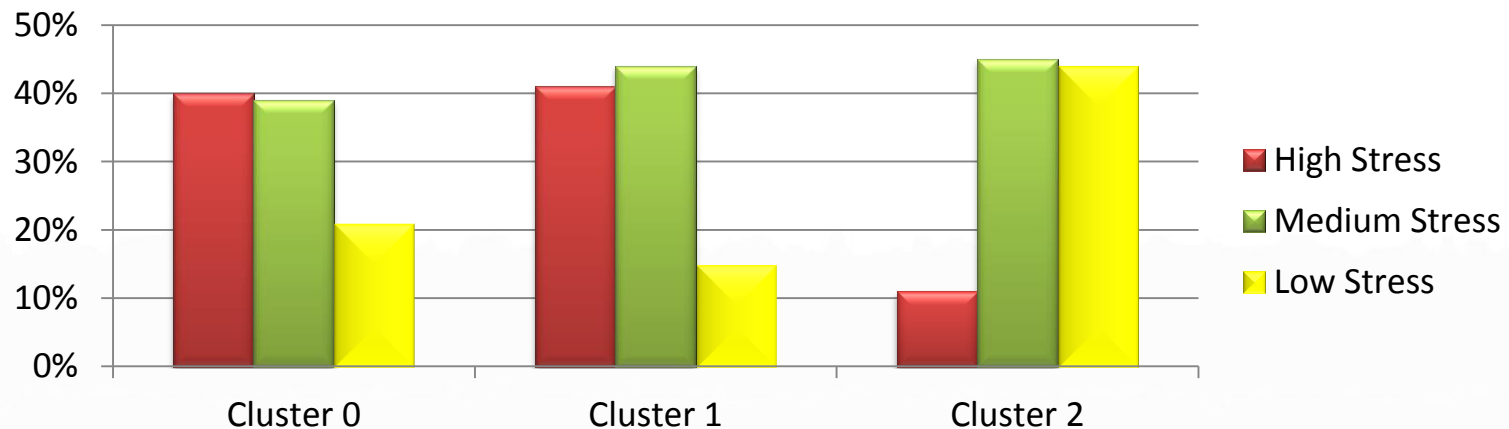


- Opt-out ability integrated, delete all user data upon selection.
- Dataset statistical analysis proved its efficiency and absence of bias.

Flat classification (overall indicators)



- Goal: extract correlations between **usage patterns** and **users who share same stress valuation** (according to BAI test).
- Transformed relational database into a **single tuple record** containing solely users' **comments** and **statuses**.
- Flat data tuple subjected to stemming process.
- EM algorithm produced 3 clusters:
 - Cluster 0 has too few users.
 - Cluster 1 includes users with high and medium-to-high stress score.
 - Cluster 2 includes users with low and medium-to-low stress score.



Chronicity analysis (indicators over time)



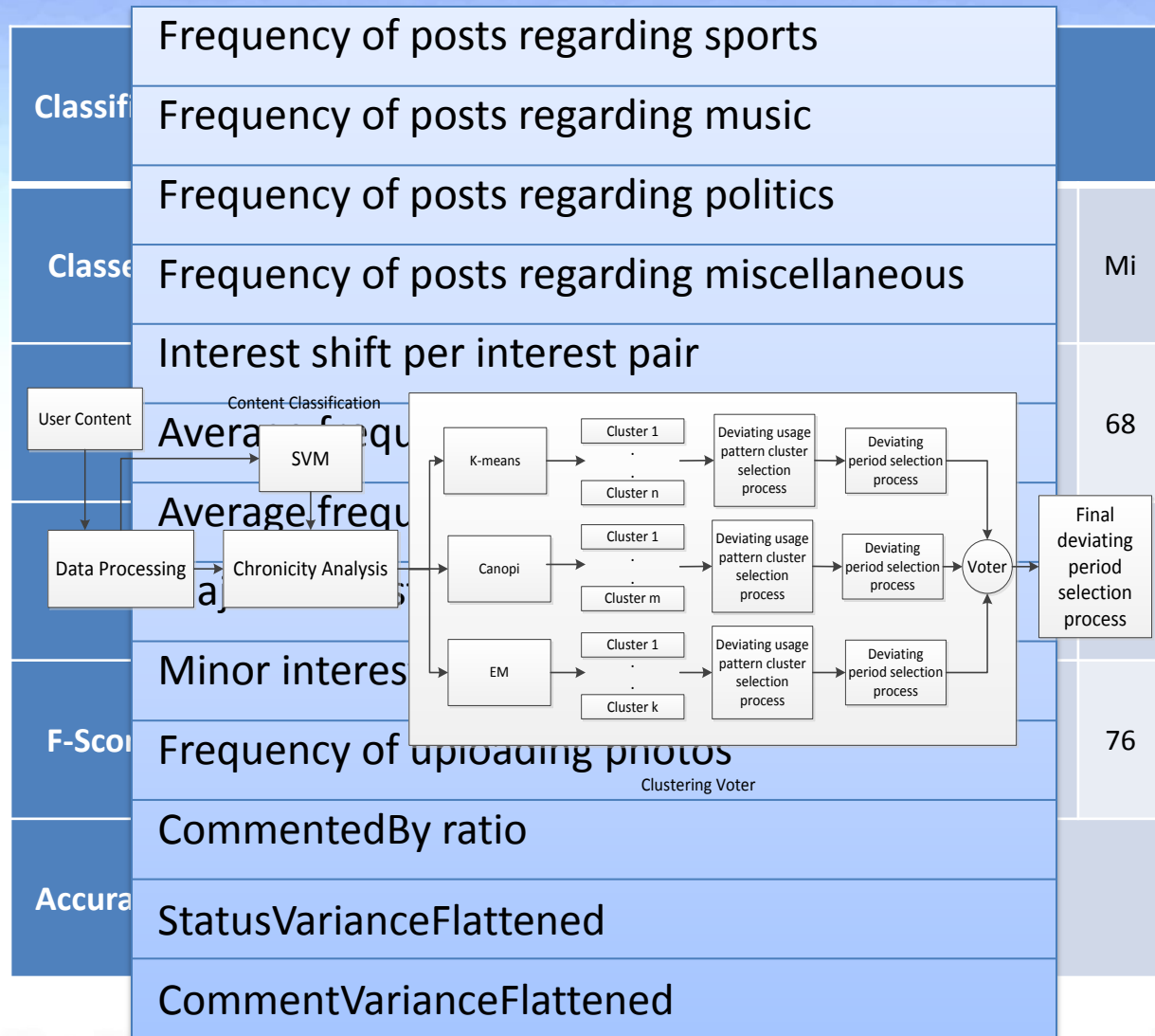
- Goal: **detect differentiations** of OSN usage patterns over **time related** to depicted stress level.
- Split users' usage pattern into time periods (from one day to one month).
 - Time period of one week produced best results.
- Chronicity analysis system consists of 2 modules:
 - Preprocessing data module (responsible for the processing of input data).
 - Usage pattern analysis module (responsible for analyzing usage patterns based on a set of metrics).
- Usage pattern fluctuations depict differentiated medium usage.

Chronicity analysis steps

Step 1: Classify user generated content into 4 predefined categories ('S' stands for sports, 'M' for music, 'P' for politics and 'Mi' for mis-cellaneous).

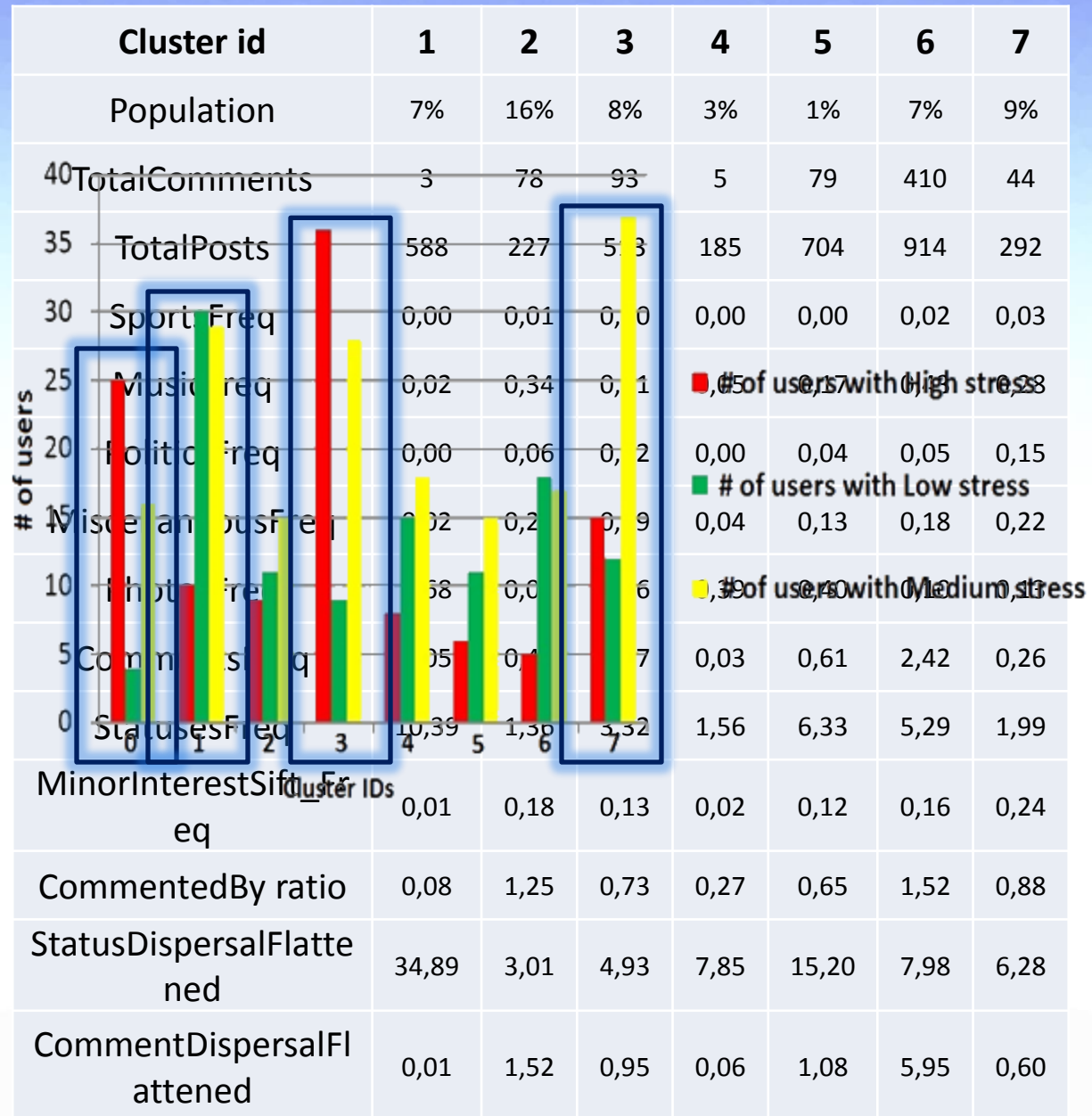
Step 2: Calculate following metrics for each user and time period (metrics developed on an ad-hoc basis according to our observations).

Step 3: Transform metrics results into arithmetic vectors and perform data mining on them using (a) *K-means*, (b) *EM*, and (c) *Canopy* algorithms. Utilize voter to decide fluctuations.



Chronicity analysis results

- Metrics results per detected cluster.
- Visual representation of users belonging to each cluster.
- **Clusters 0 and 3** contain mainly users classified in high stress category.
- In **cluster 0**, users post mainly photos.
- In **cluster 3** users post photos, discuss about music, whereas a small fraction of the content is referring to miscellaneous information.
- **Clusters 1 and 7** contain many users classified in medium or low stress category.
- **Clusters 1 and 7** refer mainly to music and miscellaneous content and also contain limited content referring to sports.




Case 4

Scope: Identifying Political Beliefs



Horror
story

OSINT		OSN: YouTube 
Tools used for the analysis		
Science	Theory	
Computing	Machine Learning	
	Data Mining	
Political Sociology		

Case 4: **Horror story** – Identifying Political Beliefs



Divided loyalty

Study: Motive, ideology, divided/reduced loyalty, predisposition towards law enforcement

Means: Machine Learning, Content Analysis, comment classification

- Same YouTube dataset.
- Political beliefs profiling-clustering.
- Three (indicative, local context based) clusters: **Radical** – **Neutral** – **Conservative**.
- Machine Learning and Content Analysis methods used.
- Analysis also based on:
 - Social Learning Theory
 - General Deterrence Theory
- Massive ethical issues.
- Goal: raise community awareness.



Horror story

Methodology

- Three (indicative) categories: **R**adical, **N**eutral, **C**onservative:
 - Assumptions are local-context-dependent (Greece, 2007-12).
 - Test case consists of an indicative subset of the local community.
 - Analysis reflects the current local political scene.
- Defined (indicative) classes:
 - **R**adical political affiliation: center-left, left, far-left.
 - **N**eutral political affiliation: neutral or non-specified political affiliation disclosed.
 - **C**onservative political affiliation: center-right, right, far-right.
- Comments classification:
 - Comments classification performed as text classification.
 - Machine trained with text examples and the category each one belongs to.
 - Assistance of field expert (Sociologist).

Analysis of results

- **Comment** classification by:
 - Naïve Bayes Multinomial (NBM)
 - Support Vector Machines (SVM)
 - Multinomial Logistic Regression (MLR)
- Each classifier's **efficiency** was compared by:
 - Metrics (%): Precision, Recall, F-Score, Accuracy
- Multinomial Logistic Regression was chosen:
 - MLR classifies appropriately a comment with 87% accuracy.
 - Use of precision, recall and f-score to further examine classifiers' efficiency.

Precision: Measures the classifier exactness. Higher and lower precision means less and more false positive classifications, respectively.

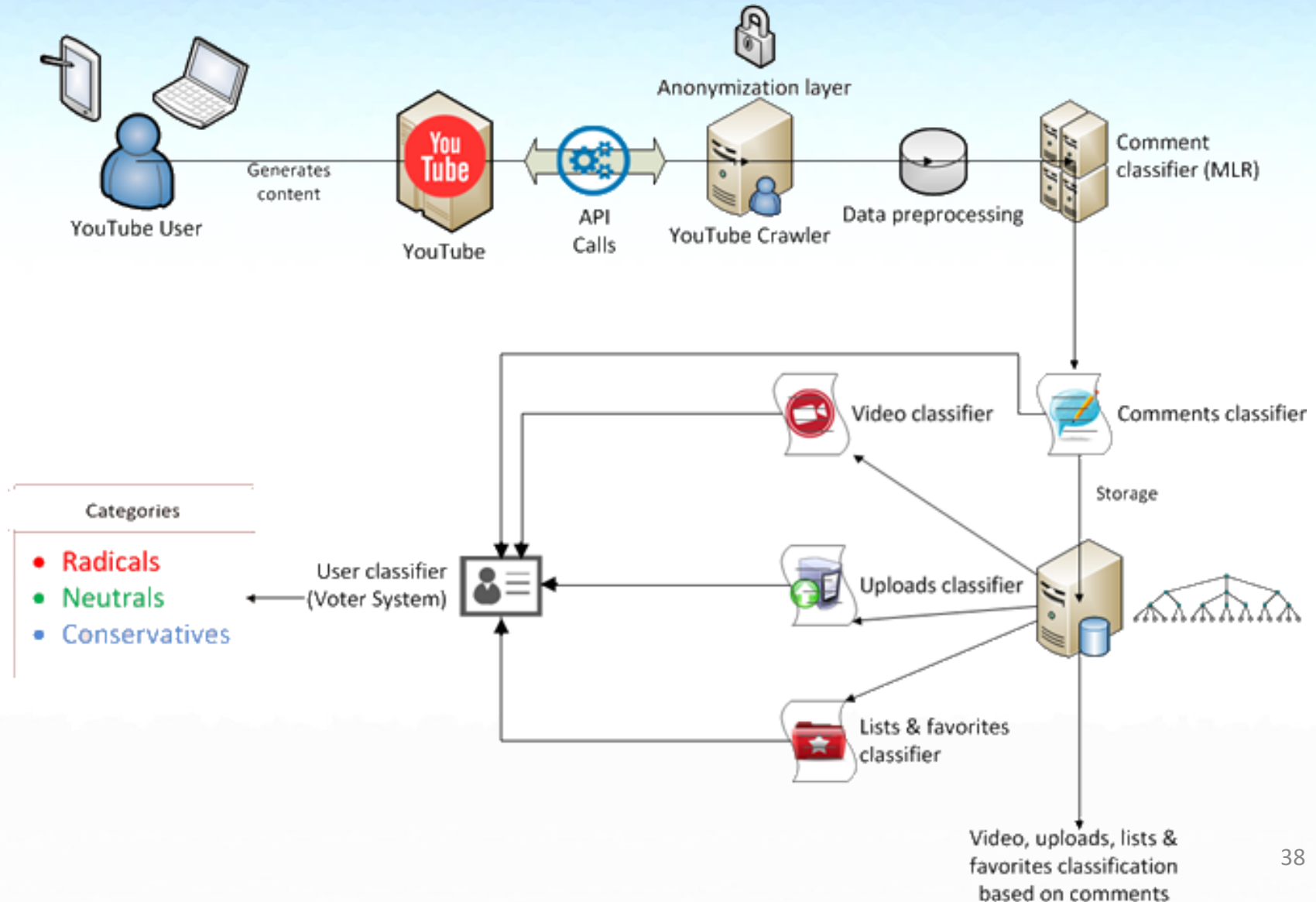
Recall: Measures the classifier completeness. Higher /lower recall means less/ more false negative classifications, respectively.

F-Score: Weighted harmonic mean of both metrics.

Accuracy: No. of correct classifications performed by the classifier. Equals to the quotient of good classifications by all the data.

Classifier	Metrics								
	NBM			SVM			MLR		
Classes	R	N	C	R	N	C	R	N	C
Precision	65	93	55	75	91	74	83	91	77
Recall	83	56	85	80	89	73	77	93	78
<u>F-Score</u>	73	70	60	76	89	73	80	92	77
Accuracy	68			84			87		

In a nutshell



Example of conclusions extraction

- Each **comment** falls into a category, based on the classifier's prediction.
- Each **video** falls into a category based on its **comments**.

Video "Example"			
Comment	Political affiliation	Likes	Dislikes
#1	R	90	10
#2	C	15	20
#3	R	30	5
#4	N	5	2
#5	R	10	3
Total		150	40

All comments are taken into account.

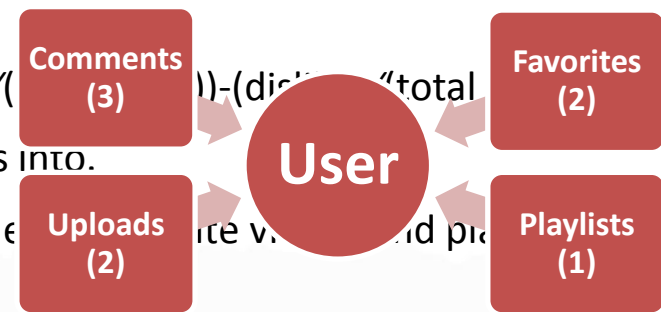
Like means "approve" and dislike means "not approve".

$$R = (1+90/150-10/40) + (1+30/150-5/40) + (1+10/150-3/40) = 4.1$$

$$C = (1+15/150-20/40) = 0.6$$

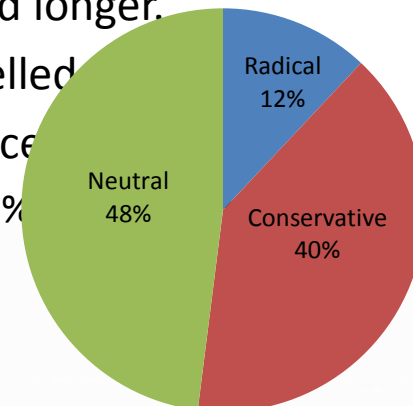
$R > C$ thus the video is classified as R

- Two sums are calculated (i.e. R,C).
- For every comment in a video we calculate: $1 + ((\text{Likes}/(\text{Likes} + \text{Dislikes})) - (\text{dislikes}/(\text{Likes} + \text{Dislikes})))$
- The greater the sum, the more the category, the video falls into.
- Same applies to list of videos, i.e. user's uploaded video user's beliefs.

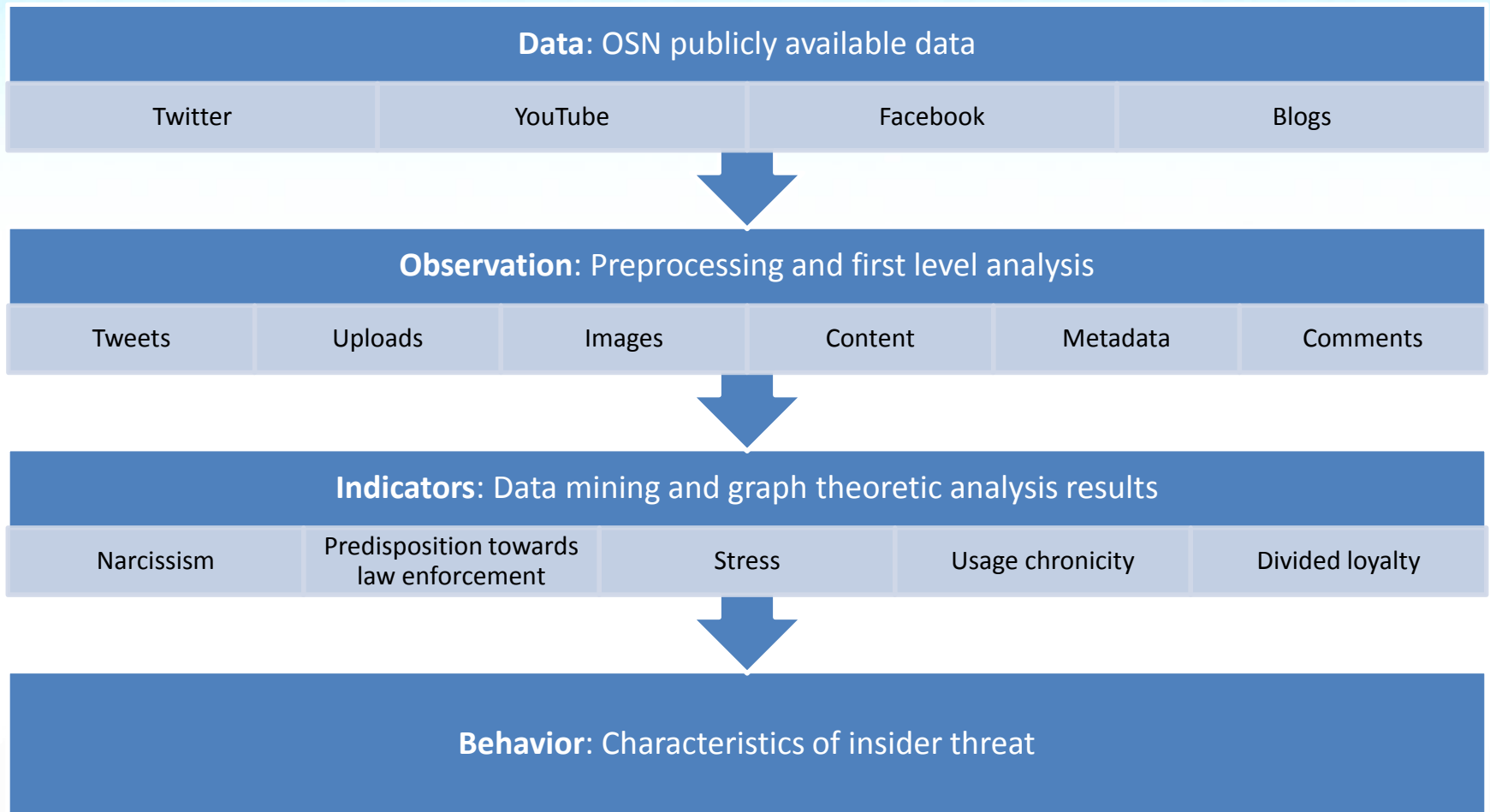


Basic observations

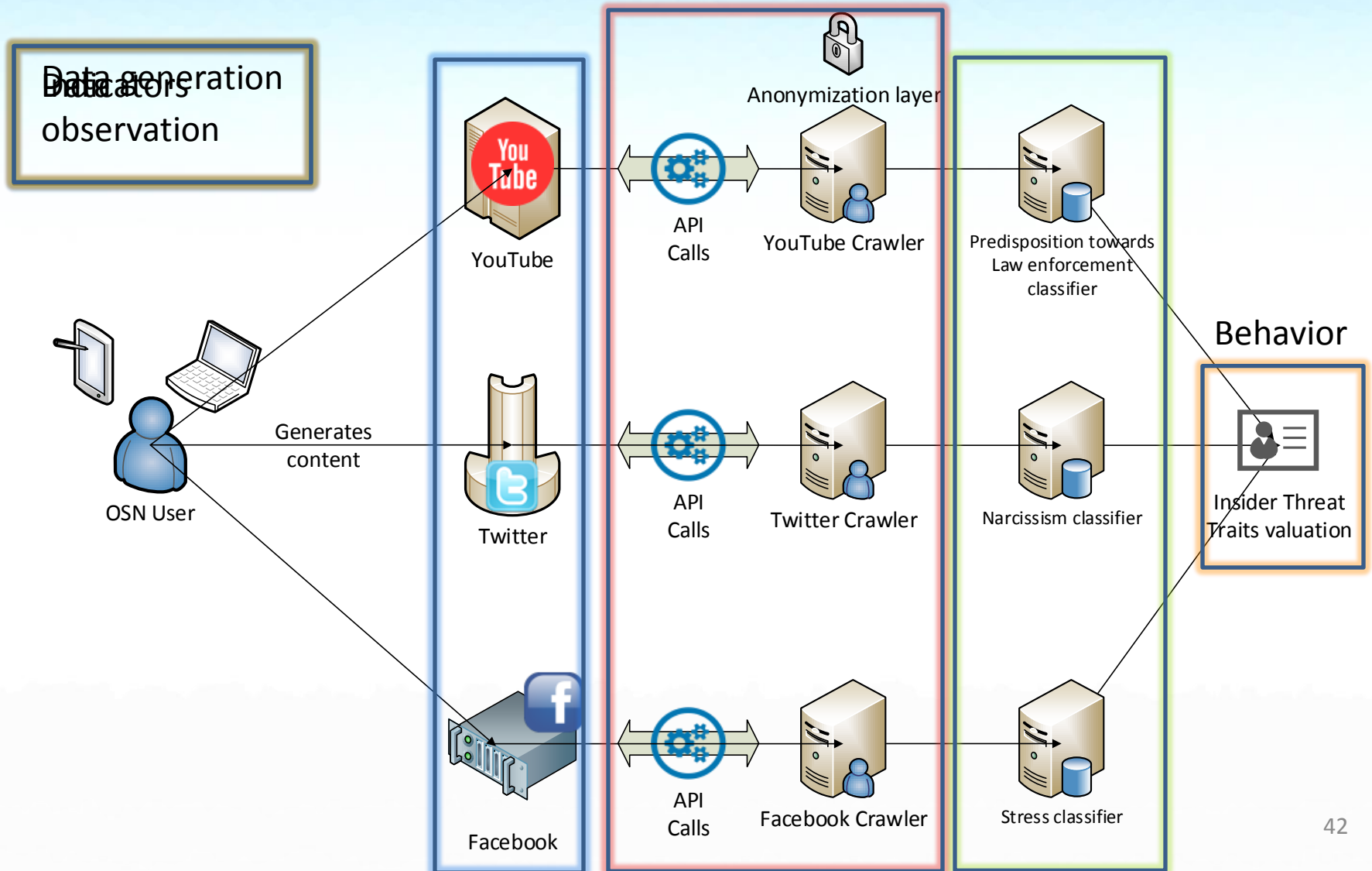
- **2% of comments** demonstrate political affiliation (0.7% Radical, 1.3% Conservative)
 - 20% of their comments includes political position.
 - 2% means that almost **41.000 comments** (of the 2.000.000 collected) include political content.
 - Prefer Greek alphabet (i.e., 54% comments in Greek, 33% in greekish, 13% use both).
 - Massively comment on specific videos.
- **7% of videos** classified into a specific category (2% Radical, 5% Conservative)
 - Prefer videos with political content (political events, music, incidents of police brutality).
 - Add to their favourites documentaries and political music clips.
- **7% of videos** classified into a specific category (2% Radical, 5% Conservative)
 - 7% means that almost 14.000 videos (of the 200.000 collected) include political content.
- **Conservatives:**
 - Prefer greekish in comments (i.e., 55% greekish, 35% Greek, 10% both).
- **12% of users** express **Radical** political affiliation and **40% Conservative** affiliation
 - Often share conspiracy-based or videos with nationalistic content.
- **52%** means that **6.760 users** reveal - one way or another - their political beliefs.
- **Radicals:**
 - Greekish comments are usually shorter and aggressive.
- **Greek comments** are usually explanatory, polite and longer.
- The more aggressive a comment - the more misspelled.
- **7% of videos** published under Creative Commons license
 - 55% uploaded by Radicals, 10% by Conservatives, 35% by Neutral.



Model for predicting threats



Visualization of the model



OSN data exploitation paths

- **Insider threat prediction:**
 - Adopting Shaw and FBI psychosocial indicators (narcissism, anger or revenge syndrome, etc.).
- **Delinquent behavior prediction:**
 - Analysis of psychosocial characteristics (narcissism, anger or revenge syndromes, etc.).
 - Predisposition analysis (graph theory and content analysis through social learning theory, etc.).
- **Forensics analysis support:**
 - Suspect profiling and analysis (proactive prediction of delinquent behavior, etc.).

Ethical and legal issues

- Users are **not** aware of the actual reach of the information they reveal.
- Some methods used for **OSINT** may:
 - be associated with discrimination,
 - infringe human rights (freedom of speech, conception of identity, privacy, etc.),
 - cause self-censorship and self-oppression and
 - pose a threat of marginalization (employers or rigid micro-societies).
- OSN often offer privacy options which **do not really** help.
- Private profiles are usually **indirectly crawlable**.
- **Laws** may not clearly prohibit the process of data revealing psychosocial characteristics.
- Derogations are often allowed:
 - On a legal manifest of public interest (e.g. critical infrastructures, security officers, etc.).
 - If given an explicit, informed and written consent of the person concerned.

Some general conclusions

- ✓ OSN produce vast amounts of **crawlable** information and OSINT may transform this information into **intelligence**.
- ✓ Security analytics can assist in detecting **narcissistic behavior**, **predisposition towards law enforcement**, **divided political loyalty**, etc.
- ✓ Security analytics can be a proactive cyber-defense tool and **predict insider threat**, **predict delinquent behavior**, **assist in law enforcement**.
- ✓ OSINT may lead to unwanted **horror stories**.
- ✓ OSINT intrusive nature dictates **limited** use, e.g. security officers selection, critical infrastructure protection.

References

1. Gritzalis D., Stavrou V., Kandias M., Stergiopoulos G., "Insider Threat: Enhancing BPM through Social Media", in *Proc. of the 6th IFIP International Conference on New Technologies, Mobility and Security (NMTS-2014)*, Springer, UAE, 2014.
2. Gritzalis D., "Insider threat prevention through Open Source Intelligence based on Online Social Networks", Keynote address, *13th European Conference on Cyber Warfare and Security (ECCWS-2014)*, Greece, 2014.
3. Gritzalis D., Kandias M., Stavrou V., Mitrou L., "History of Information: The case of Privacy and Security in Social Media", in *Proc. of the History of Information Conference*, Law Library Publications, Athens, 2014.
4. Kandias M., Mitrou L., Stavrou V., Gritzalis D., "Which side are you on? A new Panopticon vs. privacy", in *Proc. of the 10th International Conference on Security and Cryptography (SECRYPT-2013)*, pp. 98-110, Iceland, 2013.
5. Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", in *Proc. of the 7th International Conference on Network and System Security (NSS-2013)*, pp. 220-235, Springer (LNCS 7873), Spain, June 2013.
6. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security (CRITIS-2011)*, pp. 93-103, Springer (LNCS 6983), United Kingdom, 2013.
7. Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing (ATC-2013)*, pp. 347-354, IEEE Press, Italy, 2013.
8. Kandias M., Stavrou V., Bosovic N., Mitrou L., Gritzalis D., "Proactive insider threat detection through social media: The YouTube case", in *Proc. of the 12th Workshop on Privacy in the Electronic Society (WPES-2013)*, pp. 261-266, ACM Press, Germany, 2013.
9. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Workshop on Critical Infrastructure Security (CRITIS-2011)*, Bologna S., et al (Eds.), pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.
10. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., "An Insider Threat Prediction Model", in *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business (TrustBus-2010)*, pp. 26-37, Springer (LNCS-6264), Spain, 2010.
11. Mitrou L., Kandias M., Stavrou V., Gritzalis D., "Social media profiling: A Panopticon or Omnipticon tool?", in *Proc. of the 6th Conference of the Surveillance Studies Network*, Spain, 2014.
12. Mylonas A., Meletiadiis V., Tsoumas B., Mitrou L., Gritzalis D., "Smartphone forensics: A proactive investigation scheme for evidence acquisition", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 245-256, Springer (AICT 267), Greece, 2012.
13. Pipyros K., Mitrou L., Gritzalis D., Apostolopoulos T., "A Cyber Attack Evaluation Methodology", in *Proc. of the 13th European Conference on Cyber Warfare and Security (ECCWS-2014)*, Greece, 2014.
14. Stavrou V., Kandias M., Karoulas G., Gritzalis D., "Business Process Modeling for Insider threat monitoring and handling", in *Proc. of the 11th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS-2014)*, Springer, Germany, 2014.
15. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009)*, Springer, USA, 2009.
16. Theoharidou M., Mylonas A., Gritzalis D., "A risk assessment method for smartphones", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 443-456, Springer (AICT 267), Greece, 2012.