Legal Protection by Online Broker for Trade Secrets in the Cloud

Muhammad Umer Wasim

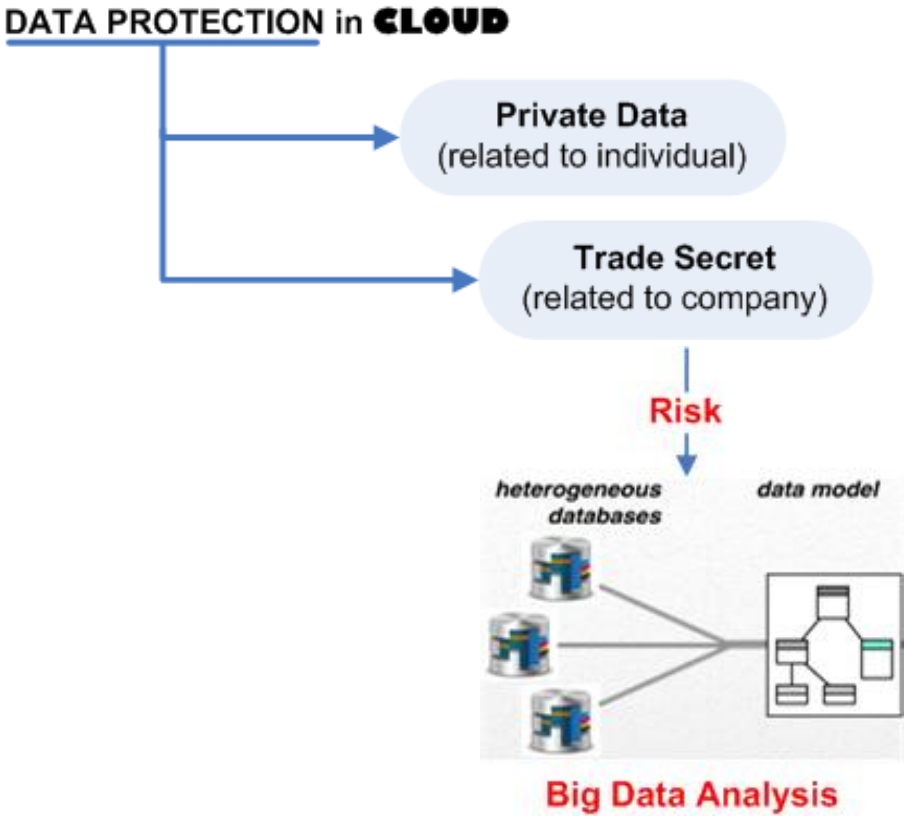
Main Supervisor: Pascal Bouvry, University of Luxembourg (Luxembourg)
Co- supervisor : Tadas Limba, Mykolas Romeris University (Lithuania)

PCOG Yearly Team Meeting
5 December 2016
Belval, Luxembourg
http://pcog.uni.lu/

About Myself

- **Education (Engineering and Computer Science)**
  - Masters in Eng. & Policy Analysis (TUDelft, Netherlands 2008)
  - Masters in Information Technology (NUST, Pakistan 2006)
  - Bachelor in Computer Science (Hajvery, Pakistan 2003)
- **Recent Experience**
  - Research Domains:
    - Cloud computing
    - Cyber law
    - Innovation Ecosystems (Science Park and Incubator)
  - Research Tools
    - Computer Programming
    - Econometrics

Problem



Can be any thing that company hides: Formula, customer list, business model, practice, process, contracts, design, instrument, pattern, commercial method, or compilation of information etc.

Q: How to protect **Trade Secret (TS)** in the Cloud when data is not public?
- Industrial Internet of Things (IIOT)

NOT TRUE when data is public
> PeopleBrowsr, Inc. v. Twitter, Inc
> Tiffany (NJ), Inc. v. eBay, Inc.

Current Progress

- Chapter 1
  - Introduction
- Chapter 2
  - Literature Review
  - Research Gap

Review Paper (Ready for Submission)

- Chapter 3
  - Proposed Methods
  - Proof of Concept

Concept paper (OR 2016)

- Chapter 4
  - Experimentation and Results

Paper (in progress)

Review Paper

- To maximize protection for TS, data protection legislation has evolved **BUT** uniformity is missing

	Criminal Law	Unfair Competition Law	Labour Law	Civil Code	IP Law	Contract Law	Tort Law	Common Law of Confidence	Specific Law on Trade Secrets	Others
Greece	x	x	x	x	x		x			x
Belgium	x	x	x	x		x	x			
France	x		x	x	x	x	x			
Romania	x	x	x	x	x					x
Austria	x	x	x		x					x
Hungary		x	x	x	x	x				
Italy	x	x	x	x	x					
Latvia	x	x	x				x			x
Netherlands	x	x	x	x			x			
Spain	x	x	x		x					x
Bulgaria		x	x	x						x
Cyprus	x	x				x				x
Finland	x	x	x							x
Germany	x	x	x							x
Lithuania	x	x	x	x						
Poland	x	x	x	x						
Slovenia	x	x	x			x				
Sweden	x							x	x	x
Denmark	x	x	x							
Estonia	x	x	x							
Republic of Ireland						x	x	x		
Luxembourg	x	x				x	x			
Portugal	x		x		x					
Slovakia	x	x	x							
Czech Republic	x	x								
Malta				x		x				
UK						x	x			

SOLUTION EC directive/Regulation

Assumption: jurisdiction for trade secret is transfixed

Review Paper

- Such regulations **fail** to protect trade secret in the Cloud because of high degree of borderless data mobility
- To build an **argument for legal protection of TS in the Cloud**, in the domain of "Case Law", precedents set by previous court rulings for protection of TS (in online/offline environment) were reviewed
- **Argument 1**: To pursue a claim for TS misappropriation, plaintiff must proof before the court of law
  - Presence: Proof of data in Cloud to be TS
  - Confidentiality: Proof of reasonable efforts made by owner to protect TS
  - Misappropriation: Proof of TS misappropriation

  Reasonable efforts to proof confidentially must include:
  - assess **Structural Significance of Criteria** (for Security)
  - Inspect contract for **compliance with non-disclosure regulations**
- **Argument 2**: As per increasing use of Cloud services and IIoT (outsourcing), confidentiality is becoming a complex phenomenon to proof. As a result, it is more suitable to certify confidentiality by using preemptive measures rather waiting for the litigation to unfold (same as privacy by design >> Confidentiality by design)

legal protection = **Preemptive measures (Structural Sig. & Compliance)**

Review Paper

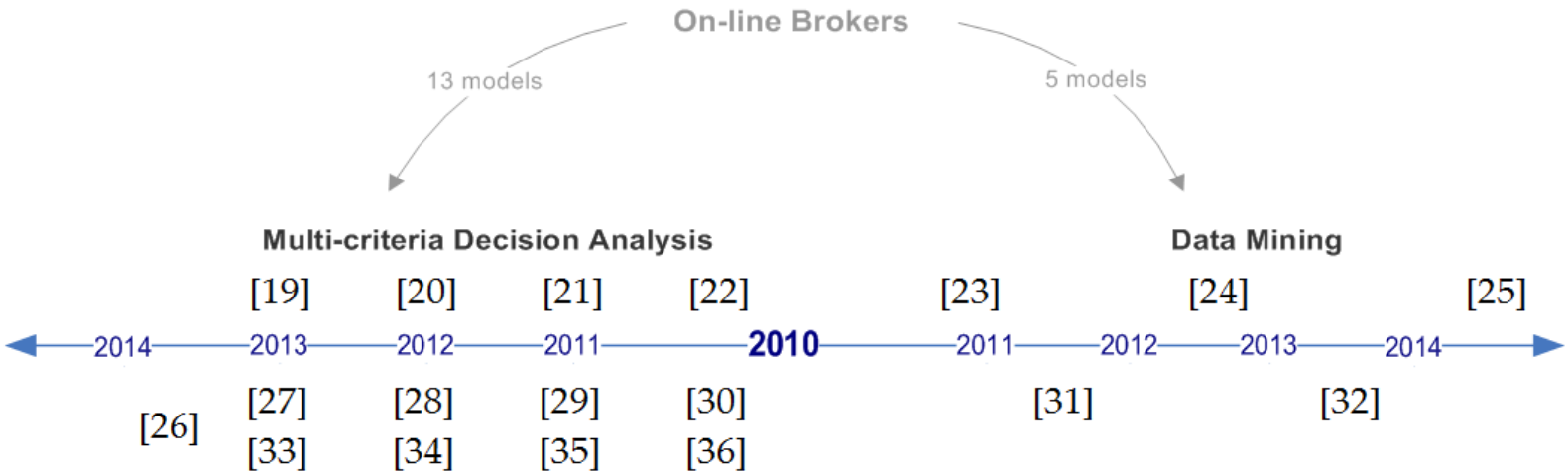
- Information Security is a domain of ICT that includes **Preemptive measures** designed to protect confidential data from unauthorized disclosure
- In the Cloud, Information Security enforcement point that is placed before Cloud service and IIoT is a software *agent* also known as **online Broker.**
- This Broker is expected to enforce preemptive measures that can certify confidentiality in the Cloud

legal protection = **Preemptive measures (Structural Sig. & Compliance)**

legal protection = **Online Broker (Structural Sig. & Compliance)**

- Example: regulations or standards compliance by Online Broker **But** what about structural significance (relevance of criteria as per given context / goal)?

Review Paper



Findings: Based on the assumption that structural significance exist: Results of most often used Multi-criteria Decision Analysis (MCDA) by online Brokers can be biased (**omitted-variable-bias**)

Conclusion: In the Cloud, above mentioned bias can question reliability of an online Broker to **certify** legal protection of a trade secret.

Future Research: Proposed model for online Broker that can assess structural significance of criteria (to be used for security)

Concept Paper (OR 2016)

- Assuming structural significance can lead to structural uncertainly
- To deal with structural uncertainty, **Self-Regulated MCDA** is proposed
  - It uses notion of "**factor loading**" that measures significance of each criterion
  - High loading indicates strong correlation and high significance of criterion to be used in a model
- Factor loading belongs to broader concept of factor analysis from the field of statistics

X = Criteria and F = Security

$$X = \lambda_i F + \mu_i \qquad (1) \qquad X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Where λ_i is the factor loading of X on F Equation 1 is not testable, since F is unobserved

However, using structural equation modeling, it is testable

Concept Paper (OR 2016)

Step 1 - Correlation Matrix

	CS	TS	EU	SS	SP	PR	RT	AV
CS	1.000	0.878	0.516	0.345	0.594	0.665	0.669	0.780
TS	0.878	1.000	0.583	0.324	0.639	0.688	0.706	0.866
EU	0.516	0.583	1.000	0.351	0.503	0.515	0.369	0.547
SS	0.345	0.324	0.351	1.000	0.479	0.440	0.160	0.221
SP	0.594	0.639	0.503	0.479	1.000	0.611	0.519	0.551
PR	0.665	0.688	0.515	0.440	0.611	1.000	0.662	0.655
RT	0.669	0.706	0.369	0.160	0.519	0.662	1.000	0.775
AV	0.780	0.866	0.547	0.221	0.551	0.655	0.775	1.000

Step 2 - R^2 Values

CS	TS	EU	SS	SP	PR	RT	AV
0.782	0.868	0.421	0.337	0.531	0.624	0.674	0.813

Step 3 - Reduced Correlation Matrix

	CS	TS	EU	SS	SP	PR	RT	AV
CS	0.782	0.878	0.516	0.345	0.594	0.665	0.669	0.780
TS	0.878	0.868	0.583	0.324	0.639	0.688	0.706	0.866
EU	0.516	0.583	0.421	0.351	0.503	0.515	0.369	0.547
SS	0.345	0.324	0.351	0.337	0.479	0.440	0.160	0.221
SP	0.594	0.639	0.503	0.479	0.531	0.611	0.519	0.551
PR	0.665	0.688	0.515	0.440	0.611	0.624	0.662	0.655
RT	0.669	0.706	0.369	0.160	0.519	0.662	0.674	0.775
AV	0.780	0.866	0.547	0.221	0.551	0.655	0.775	0.813

Step 4 - Eigenvalues and Eigenvector

	4.176	0.527	0.149	0.047	-0.046	-0.075	-0.097	-0.171
CS	0.403	0.101	0.334	-0.616	0.375	-0.376	-0.225	0.060
TS	0.429	0.155	0.442	-0.134	-0.380	0.637	0.140	-0.092
EU	0.287	-0.264	0.306	0.617	0.240	0.016	-0.521	-0.207
SS	0.193	-0.659	-0.057	-0.139	0.046	-0.110	0.467	-0.523
SP	0.330	-0.374	-0.158	-0.018	-0.639	-0.297	-0.216	0.428
PR	0.366	-0.187	-0.457	-0.006	0.474	0.444	0.077	0.440
RT	0.356	0.387	-0.597	-0.049	-0.141	-0.030	-0.266	-0.523
AV	0.406	0.370	0.075	0.446	0.052	-0.393	0.562	0.145

Step 4 - Loading and Communalities

	CS	TS	EU	SS	SP	PR	RT	*AV*
$\wedge$	0.875	0.931	0.624	0.419	0.717	0.796	0.772	0.881
$\wedge^2$	0.766	0.866	0.389	0.176	0.515	0.633	0.596	0.776
Rk	3	1	7	8	6	4	5	2

Step 5 - Loading and Communalities
(Excluding SS with communality 0.176 <0.25)

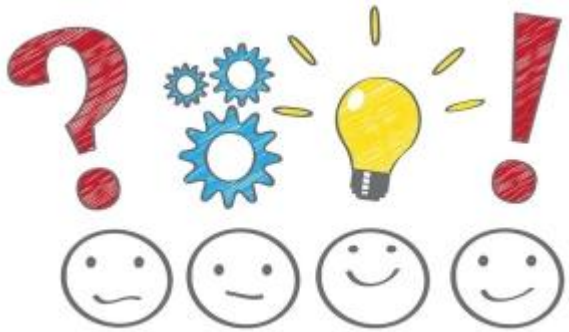
	CS	TS	EU	SP	PR	RT	AV
$\wedge$	0.877	0.938	0.614	0.693	0.780	0.786	0.869
$\wedge^2$	0.770	0.879	0.377	0.481	0.609	0.618	0.802
Rk	3	1	7	6	5	4	2

Explained Variance (%) = 0.983

Research Output & Mobility

- Mathematical Model and Software Prototype
- Why Innovative?
  - Online IPR protection & Confidentiality by Design
- Second Year
  - 3rd Term: Mykolas Romeris University (Lithuania)
  - 4th Term: University of Luxembourg (Luxembourg)
- Third Year
  - 5th & 6th Term: University of Luxembourg (Luxembourg)

Many thanks for the attention



umer.wasim@gmail.com

Confidentiality

- Confidentiality (ICT): Rules that limits access on certain types of information e.g. encryption, authentication, access controls
- Confidentiality (Case Law): Proof of reasonable efforts made by owner to protect confidential data
- What "reasonable effort" means?
  - assess **Structural Significance of Criteria** (for Security)
  - Inspect contract for **compliance with non-disclosure regulations**