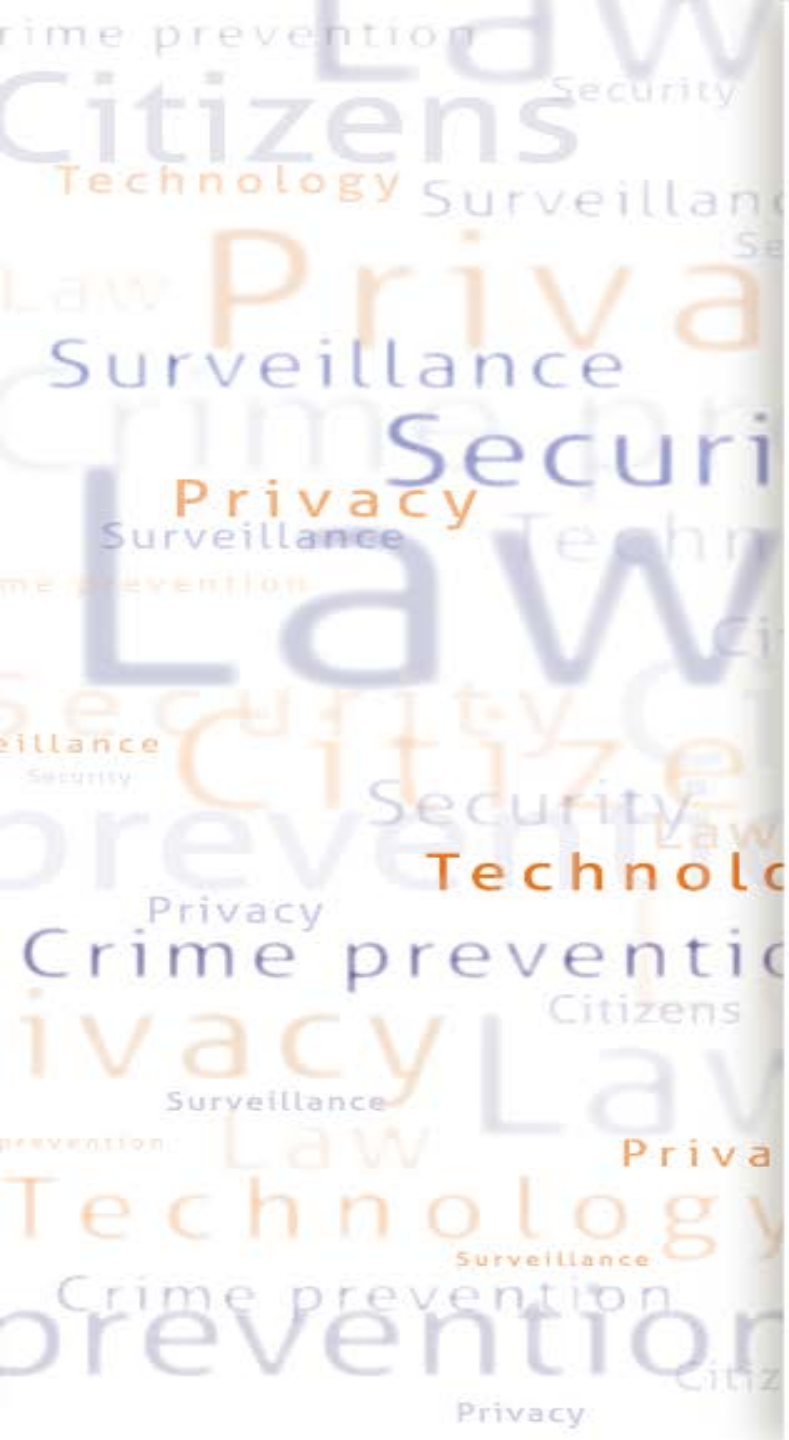


RESPECT

Rules, Expectations & Security through
Privacy-Enhanced Convenient Technologies

Surveillance of financial transactions and data protection

International Summer School in Rovaniemi 2014;
August 25-29

Erich Schweighofer, Janos Böszörmenyi

University of Vienna

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

http://respectproject.eu

Outline

- Threats to security: solution surveillance?
- Footprints everywhere, with the aim to be analysed … big data, cloud computing, Internet of Things
- Danger for privacy and data protection
- Privacy by design as a solution
- Case study: financial transactions
  - Reasons for surveillance of financial transaction to combat crime
  - Anti-Money Laundering Directive – 4th AMLD
  - New challenges for tracking financial transactions
  - Tools to comply

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Threats to international and national security

- Terrorism (e.g. Al Qaida, IS)
- Regional conflicts
- Globalisation
- Organised crime, more and more global
- Global village: real world does not notice much about global life

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Surveillance (1)

- Monitoring of activities of people in order to gather information for a particular purpose [Wikipedia EN, 22 August 2014]
  - Social control, watching threats like terrorism
  - Influencing, managing, directing, or protecting
  - Positive or negative depends on purpose and methods
  - Origin: French word for “watching over”
- Video / CCTV
- Control points, e.g. borders, airports
- Mobile phones
- Cyberspace, Social Web, Internet of Things
- Financial transactions
- Re-use of private data collections (e.g. data retention obligations)
- Sharing data (e.g. data exchange between police authorities or intelligence agencies)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Surveillance (2)

- NEW: move to smart surveillance
  - Use of AI techniques for automated analysis of information (video surveillance, pictures, data-mining, machine learning etc.)
  - More spaces, more people etc.; main constraint: quality of automated analysis is not sufficient yet

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Integrated CCTV with smart video analytics

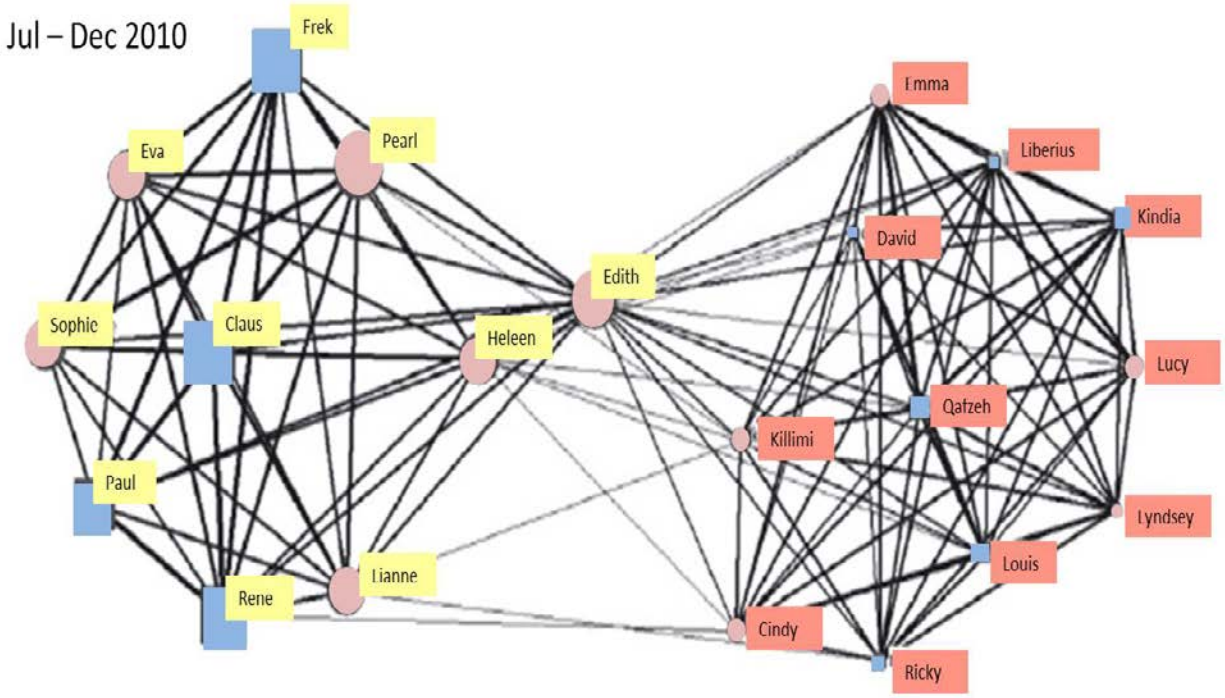
RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

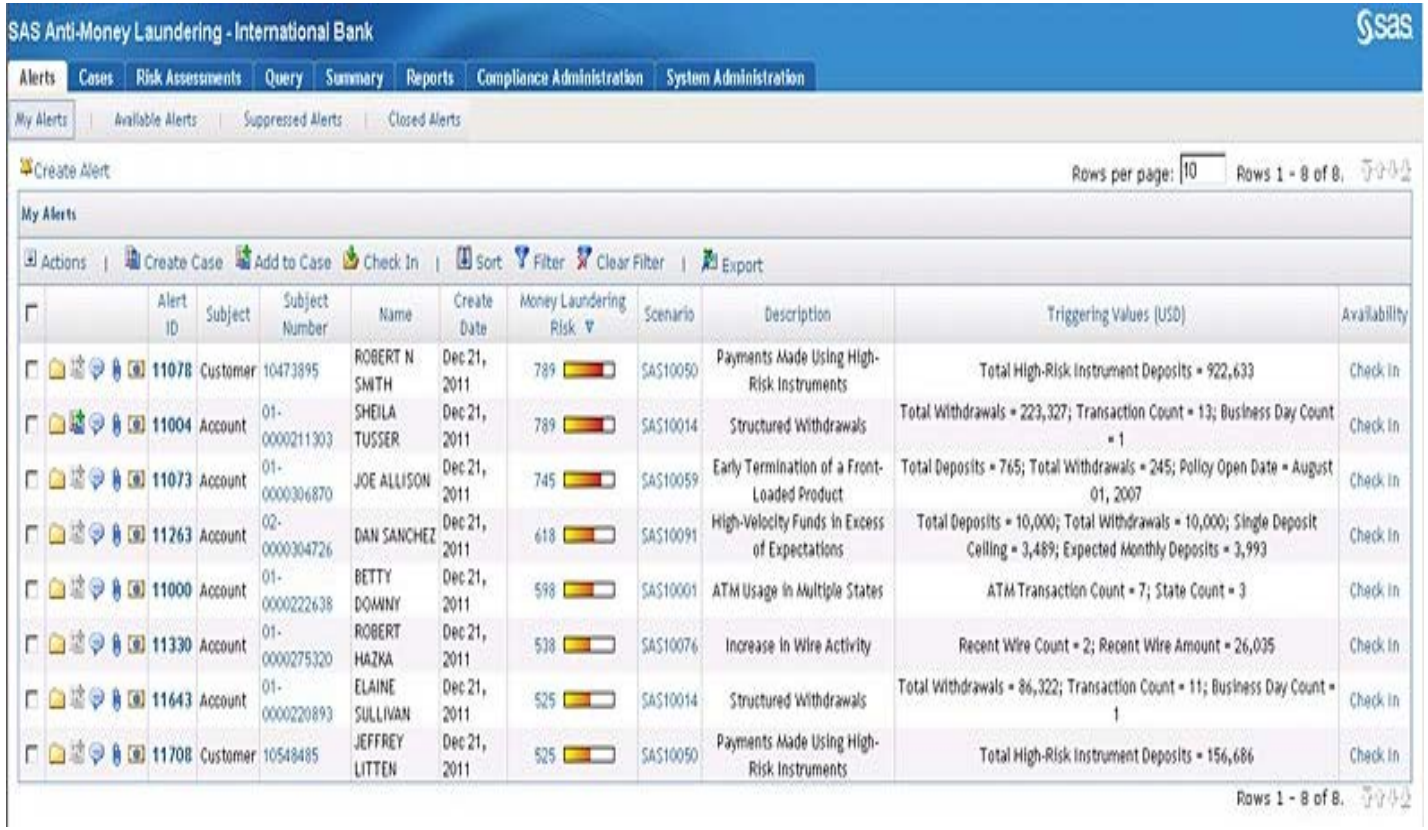
Positioning and tracking technologies

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.



Social media surveillance

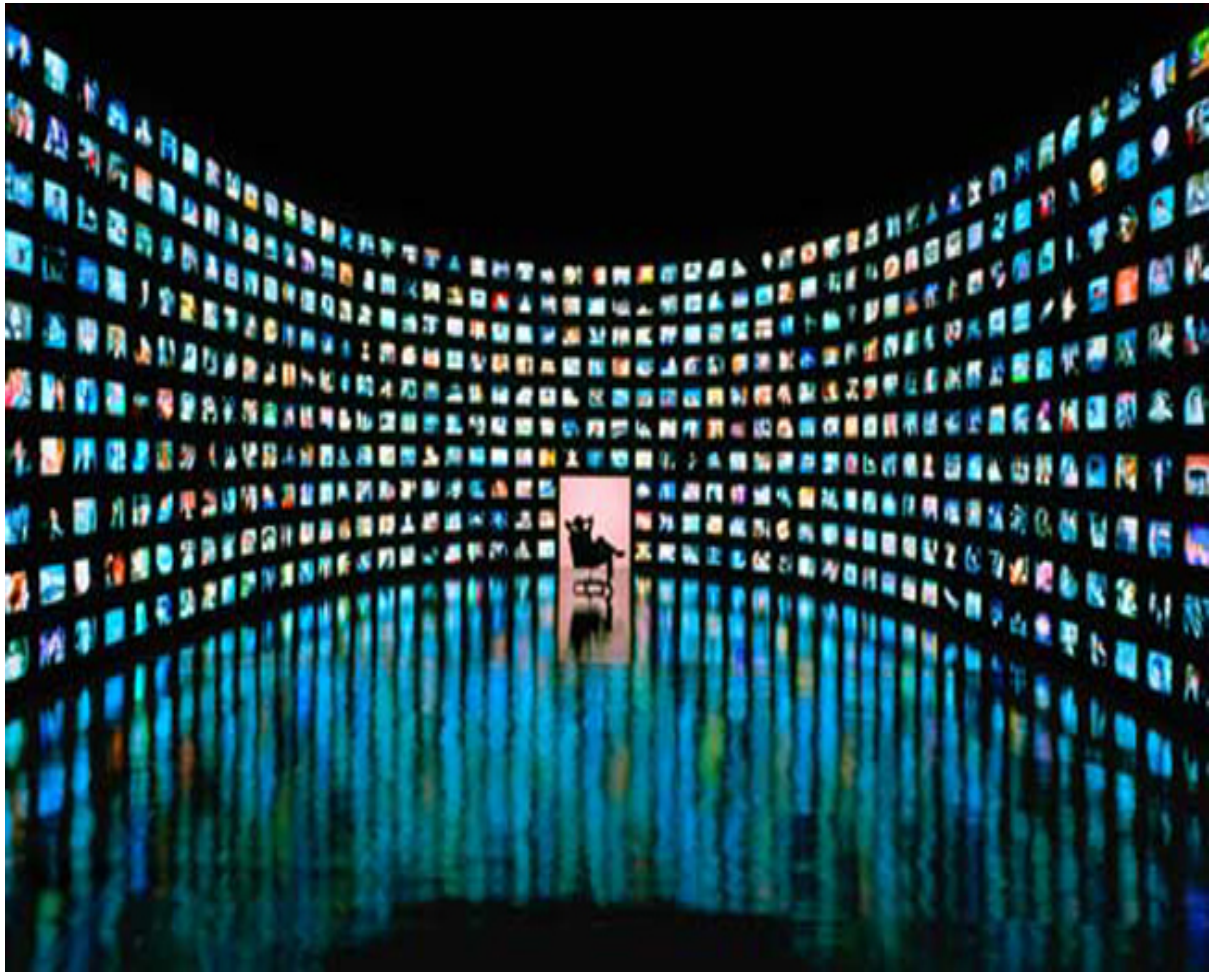
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.



Financial tracking systems

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.



Data storage, matching and mining

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

High work load …but shared now

- Public space surveillance
  - Police, private detectives, privates etc. watch public space
  - Use of automated means for gathering information (pictures, audios, videos, personal identifiers, etc.) and analysing information
  - Virtual space (Internet) surveillance
  - Enormous amount of information is collected automatically (log files etc.)
  - Data-mining techniques allow (semi)automated analysis of these data
- Private space surveillance
  - E-mails, telephone
  - Mobile devices
  - Social Web, Internet
  - Private video surveillance
  - Internet of Things

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

ICT surveillance: phone, computer, telecommunication (+ postal services) (1)

- Monitoring of communication, in particular telephone and data and traffic on the Internet
  - USA - Communications Assistance For Law Enforcement Act
    - All phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.)
  - ~~EU: Data Retention Directive~~
- Too much data requires smart, e.g. automated analysis methods
    - Text corpus analysis (e.g. certain "trigger" words or phrases), selection of websites, suspicious individuals or groups
  - Speech-to-text software

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

ICT surveillance: phone, computer, telecommunication (+ postal services) (2)

- Exploring communication tools, in particular PCs, laptops, mobile phones etc.
- Geographical location of a mobile phone
- Phone as a listening device: remotely activate the microphones in cell phones

- Postal services
  - Diminishing importance but (sic!) still higher legal constraints

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Surveillance cameras (1)

- CCTV = closed-circuit television
- Video cameras used for observing a particular place, a street, a house or a room
- Recording device, very often liked to a network
- Use is dramatically increased over the last 10 years
- Simple and cheap, e.g. home security systems or everyday surveillance possible
- Analysis: intellectual (security officer) or (semi)automatic
- Digital video footage (+ motion sensors) = searchable database + video analysis software + link-up of cameras (centralised networks of CCTV watching public areas)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Surveillance cameras (2)

- Big users
  - USA
    - Department of Homeland Security, cities etc.
  - United Kingdom
  - China
    - Golden Shield Project

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Social network analysis, biometric surveillance & identification (1)

- Social network analysis
  - Social network "maps" based on data from social network sites (Facebook, Google+, Twitter, Xing, LinkedIn, phone call records etc.)
    - Data mining techniques for extraction of information: personal data and interests, friends, contacts, affiliations, activities, interests, thoughts, wants, etc.
      - USA: fight against terrorism
- Biometric surveillance & identification
  - Technologies for measuring and analysing human physical and/or behavioural characteristics for authentication, identification, or screening

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Social network analysis, biometric surveillance & identification (2)

- Fingerprints, palm prints, DNA, facial patterns, gait (a person's manner of walking), voice, iris/retina (eye) data
- Improvement of video surveillance by automated analysis of data by facial recognition systems

- Documents (identity card, passports etc.)
- Secure documents with link to biometric data and RFID chips
- RFID tagging

- Radio Frequency Identification (RFID)
  - RFID tags: very small electronic devices, extremely inexpensive, that can be tracked (e.g. read) using radio waves from several meters away
  - Personal documents (passports)
  - Human bodies (very strong data protection concerns)
  - Things (parcels, products, etc.)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Aerial surveillance and satellite imagery, human operatives, location surveillance

- Aerial surveillance and satellite imagery
  - Visual imagery or video, gathered from the air (airborne vehicles like a plane or a helicopter, micro air vehicles (MAV) etc., satellites)
- Human intelligence
  - Undercover agents and informants
- Location surveillance
  - GPS (Global Positioning System)
  - Mobile phones
  - Social networks (Facebook, Google+ etc.)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Other surveillance techniques

- Online surveillance (trojaner)
- Hidden electronic devices ("bugs") for capturing, recording, and transmitting data
- License plate recognition

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Counter surveillance

- Practice of avoiding surveillance or making surveillance difficult
  - Recognition of license plates: get around by bicycle or on foot or using public transport with single tickets (not with a subscription if there are permanent controls).
  - Localisation by mobile phone: remove battery / not having a phone
  - Payments by credit card, cash withdrawals at ATMs: use cash.
  - Facial recognition systems: looking to the ground with a slight angle and wear a hat might fool the system
  - Communicate by email: encryption
  - Surfing the web while logged: Interacting with software solutions such as TOR

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Big Data

- Data analysis with huge data sizes, e.g. many petabytes of data in a tolerable time
  - 1 PB = 1000000000000000B = 10^{15}bytes = 1000 terabytes = 1000 gigabytes
  - Human brain: about 2.5 petabytes of binary data
- Big science
- Obama Administration 2012: Big Data Research and Development Initiative
  - NSA – Utah Data Center
- Amazon, eBay, Walmart, Fico Falcon Credit Card Fraud Detection System, Windermere Real Estate
- Big Data software
  - Hadoop (Apache), MongoDB, Splunk
- Cause vs. correlation

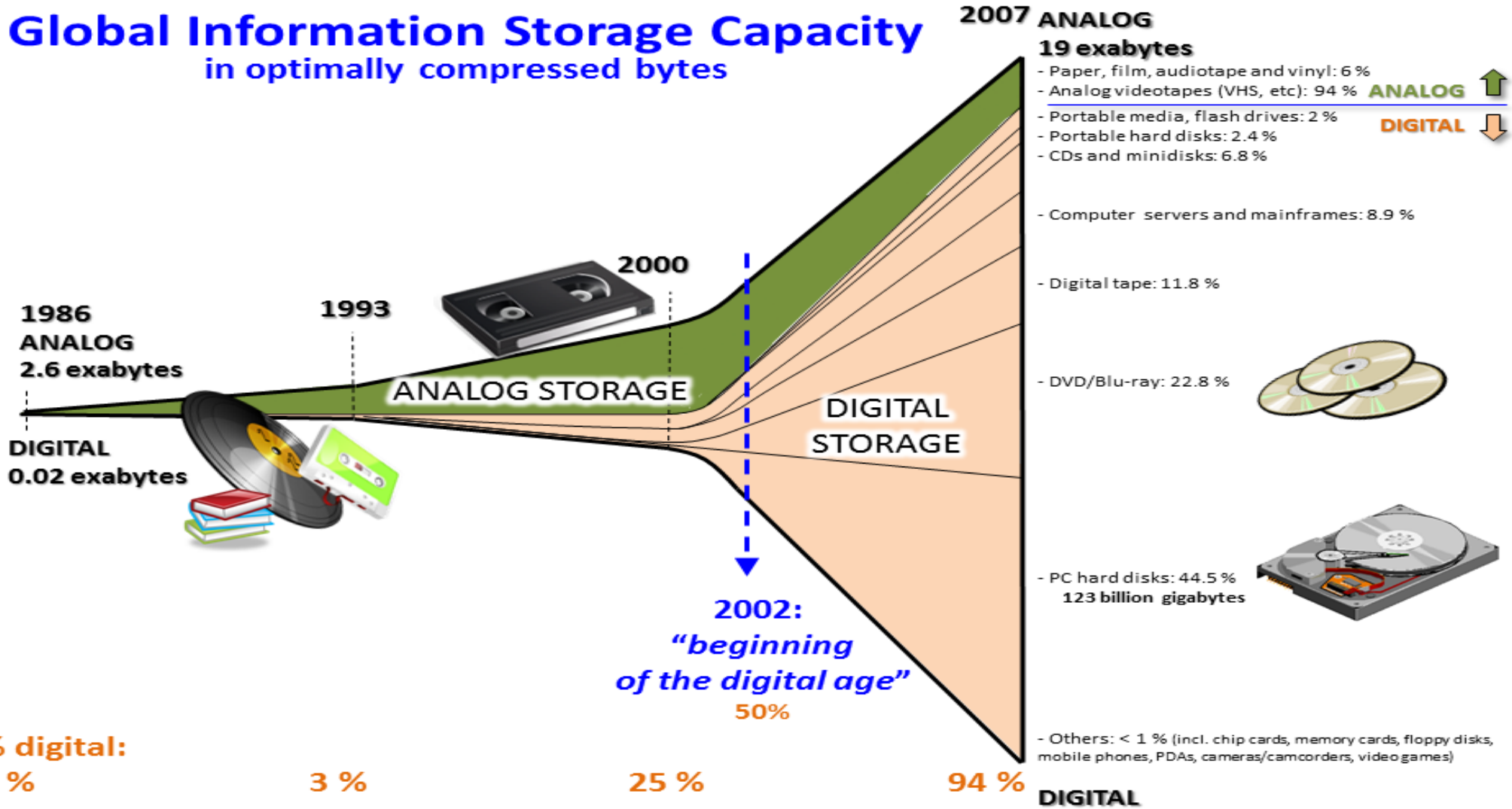
- http://en.wikipedia.org/wiki/Big_data

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Global Information Storage Capacity

in optimally compressed bytes



2007 **ANALOG**
19 exabytes

- Paper, film, audiotape and vinyl: 6 %
- Analog videotapes (VHS, etc): 94 % **ANALOG**

DIGITAL

- Portable media, flash drives: 2 %
- Portable hard disks: 2.4 %
- CDs and minidisks: 6.8 %
- Computer servers and mainframes: 8.9 %
- Digital tape: 11.8 %
- DVD/Blu-ray: 22.8 %

- PC hard disks: 44.5 %
  123 billion gigabytes

- Others: < 1 % (incl. chip cards, memory cards, floppy disks, mobile phones, PDAs, cameras/camcorders, video games)

DIGITAL
280 exabytes

Source: Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, 332(6025), 60 –65. http://www.martinhilbert.net/WorldInfoCapacity.html

RESPECT

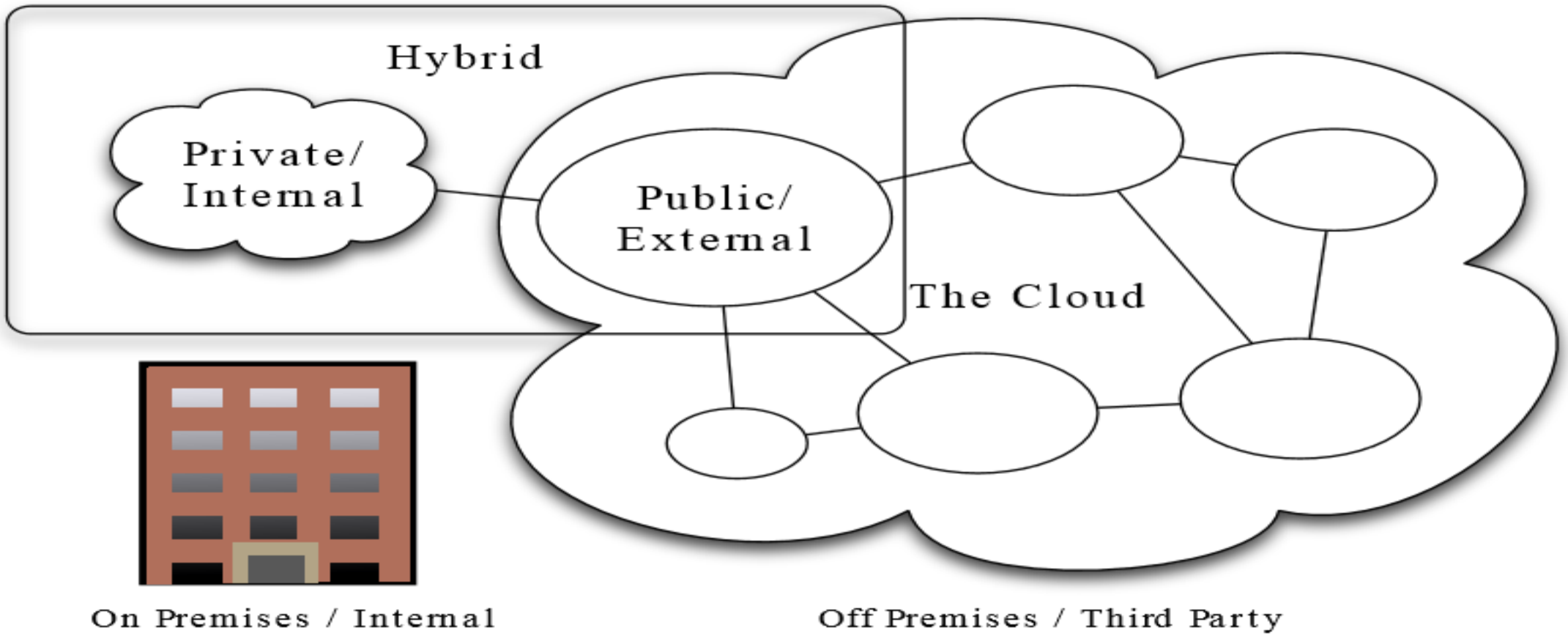
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Cloud Computing

- Hosted services (e.g. application service provisioning)
- Client server software at a remote location
  - SaaS: Software as a Service
  - PaaS: Platform as a Service
  - IaaS: Infrastructure as a Service
  - HaaS: Hardware as a Service
  - EaaS: Everything as a Service
- End user: web browser, thin client or mobile app
- Business software and user's data: stored on servers at a remote location
  - Amazon Web Services, Google App engine
- Big providers
  - Amazon, Google, Microsoft, Oracle Cloud, IBM SmartCloud etc.

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.



Cloud Computing Types

http://en.wikipedia.org/wiki/File:Cloud_computing_types.svg

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Internet of Things

- All objects (and people) are uniquely identifiable in an Internet-like structure
    - http://en.wikipedia.org/wiki/Internet_of_things
    - D2D (Device to Device) communication
- Tagging of things
    - RFID (Radio-frequency identification)
    - NFC (Near Field Communication)
    - Barcodes
    - QR codes
    - Digital watermarking

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Data mining and profiling

- Data mining
  - Application of AI techniques (statistics, neural networks, machine learning etc.) to discover relationships within the data corpus
- Data profiling
  - Same techniques but focused on assembling information about a particular individual or group
  - Sources: internet, social network, telephone, e-mails etc.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Who is doing it?

- Public surveillance
  - Government and official authorities for internal and external security
- Private surveillance (or corporate surveillance)
  - Corporations and other institutions, most often for marketing purposes
  - Very often: shared with public institutions
  - Google, Yahoo, Facebook etc.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Technical constraints

- Data storage: no
- Data collection: as such: no, intelligent data collection: yes
- Computational power: not much
- Intelligent analytics: much is happening (e-discovery)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Legal constraints

- Data protection law
- Special regulatory regimes, in particular: police, intelligence organisations, international co-operation
- Informational self-determination vs. public purpose (security concerns)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Right to data protection & privacy (1)

- Art. 8 para. 2 ECHR - right to privacy and family life

  "1. Everyone has the right to respect for his private and family life, his home and his correspondence.

  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. "

- Art. 8 EU Charter of Fundamental Rights – protection of personal data

  "1. Everyone has the right to the protection of personal data concerning him or her.

  2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Right to data protection & privacy (2)

3. Compliance with these rules shall be subject to control by an independent authority."

- Austrian Data Protection Act
  - "Sect. 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject [Betroffener].
  - (2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8, para. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data [Verwendung von Daten] that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Right to data protection & privacy (3)

- (3) Everybody shall have, insofar as personal data concerning him are destined for automated processing or manual processing, i.e. in filing systems [Dateien] without automated processing, as provided for by law,
- 1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;
- 2. the right to rectification of incorrect data and the right to erasure of illegally processed data.
- (4) Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2.
- (5) Will be repealed with 31 December 2012 by Federal Law Gazette (BGBl.) I 51/2012).
  - (5) The fundamental right to data protection, except the right to information [Auskunftsrecht], shall be asserted before the civil courts against organisations that are established according to private law, as long as they do not act in execution of laws. In all other cases the Data Protection Commission [Datenschutzkommission] shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned."

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Right to data protection & privacy (4)

- Informational self-determination
  - German Federal Constitutional Court, ruling relating to personal information collected during the 1983 census, BVerfGE 65, 1).
  - "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."
- IT privacy
  - German Federal Constitutional Court, ruling relating to on-line investigation, 27 February 2008, (1 BvR 370/07, 1 BvR 595/07)
  - Protection of data stored or processed in IT systems (part of personality right)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Right to data protection & privacy (5)

- Interference only in case of important reasons (real danger for outstandingly important legally protected interests)
- Subsidiary to rights of secrecy of telecommunications and sanctities of the home
- Fundamental right to guarantee of confidentiality and integrity of IT systems *(colloquially IT-Grundrecht, Computer-Grundrecht or Grundrecht auf digitale Intimsphäre)*

- *ECJ 9 November 2012, C 92/09, C 93/09, Volker und Markus Schecke und Eifert [transparency of agriculture subsidies]*
- *ECJ 8 April 2014, Joint Cases C 293/12 and C 594/12, Digital Rights Ireland, Kärntner Landesregierung, Seitlinger, Tschohl et al.*
- *ECJ 13 May 2014, C 131/12, Google Spain and Google*

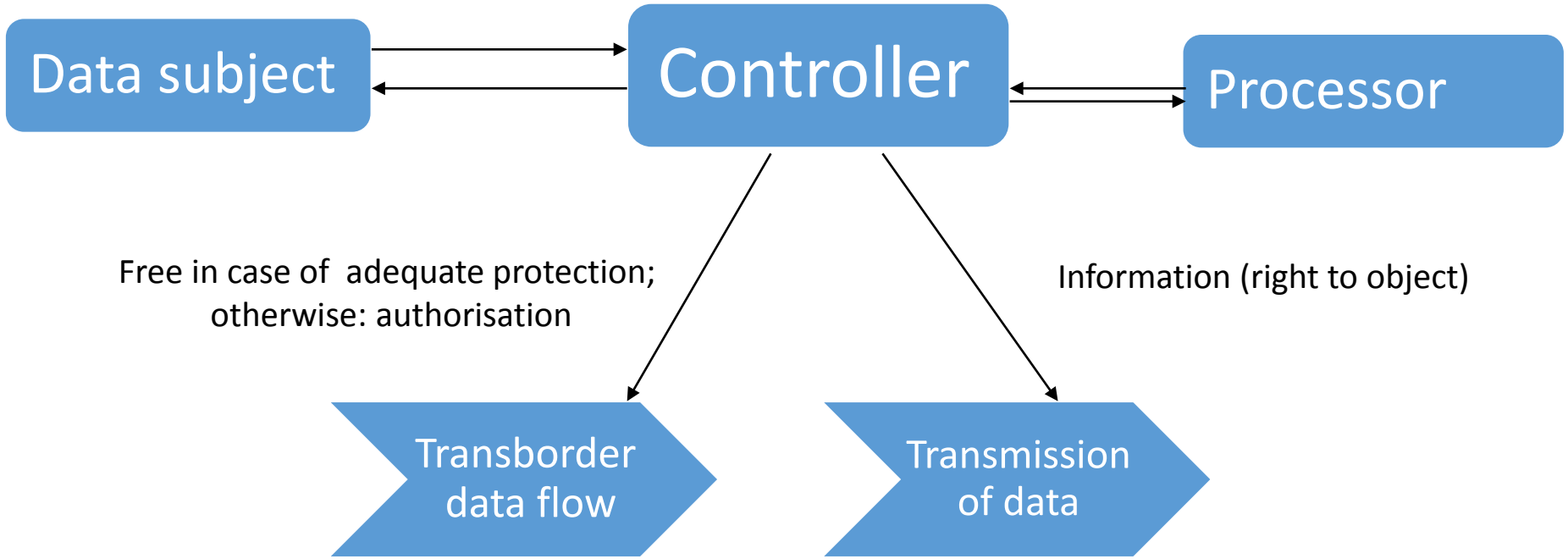
RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Model of data protection
EC Data Protection Directive (1)

Rights/Obligations: information, right of access, right to object

Filing system: any structured set of personal data which are accessible according to specific criteria



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Model of data protection
EC Data Protection Directive (2)

Controller

Legitimate purposes

Consent
- Agreement
- Performance of a contract
- Compliance with a legal obligation
- Vital interests of related person

Law
- Performance of a task carried out in the public interest or in the exercise of official authority

Principle of proportionality
- Purposes of the legitimate interests, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Case study: financial transactions

- Move to pecunia ~~non~~ olet (freely modified after Vespasian) due to money laundering, corruption, fraud, tax fraud
- Discouraging the use of real money or virtual money
- Financial transactions with full disclosure of sender, recipient, purpose, money transfer; standardised form to be easily analysed
- Identification of actors, special actors (politicians), suspects, suspicious transactions
- Privacy lost or Privacy by design solutions?

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Introduction Case Study

- EU FP7 **RESPECT Project**: Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies

- **Anti-Money Laundering** (AML), **Combating the Financing of Terrorism** (CFT), **Fraud** and **Tax crimes** (tax evasion, tax fraud)

- Money Laundering (ML) is the **intentional** conversion or transfer of property, knowing that such property is derived from **criminal activity** for the **purpose of concealing or disguising** the **illicit origin** of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.
  - Criminal activity (= **predicate offence**) is generally a prerequisite for ML
  - The aim of AML legislation is to ensure that crime does not pay and to protect the financial system

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Initial reason & catalyser

Source: http://wall.alphacoders.com/big.php?i=258026&lang=German last accessed 07.04.2014

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Predicate Offences (1)

- Terrorism
- Trafficking of illicit drugs, narcotics and psychotropic substances
- Participation in a criminal organisation
- Trafficking in human beings
- Corruption

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Predicate Offences (2)

- Weapons trafficking
- Cybercrime
- Tax crimes (offences) related to direct taxes and indirect taxes (4th AMLD)
- All offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, in case there is a minimum threshold for a minimum of more than six months (**serious crime**)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Estimates in the report on organised crime by the European Parliament's Special committee CRIM

- 3 600 international criminal organisations are operating in the EU
- Criminal organisation cause yearly up to EUR 670 billion costs to business
- Corruption costs yearly EUR 120 billion
- Trafficking in human beings generates annually a profit of EUR 25 billion
- Cybercrime causes annual losses as high as EUR 290 billion
- Loss off millions of legitimate jobs and billions in taxes (MEP Dunn)
- Approx. 330 billion euros are laundered yearly in the EU

(SWD(2013) 21 final, p.12; an estimate of the EU Commission based on reports by the IMF and UNODC)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Global and European co-operation

- Due to the ease with which money can cross borders, international co-operation is viewed as essential to combat money laundering and the financing of terrorism.
- The main international standards setting body is the FATF. Its 40 Recommendations on AML/CFT are acknowledged by the FSB as one of 12 key international standards for sound financial systems.

  - G7(G8), G20
  - Financial Stability Board (FSB)
  - Financial Action Task Force (FATF)
  - Organisation for Economic Co-operation and Development (OECD)
  - United Nations, in particular UNODC (United Nations Office on Drugs and Crime)
  - Egmont Group of Financial Intelligence Units
  - INTERPOL
  - Council of Europe (MONEYVAL Committee)
  - European Union

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

FATF comprises of 34 Member Jurisdictions and 2 Regional Organisations

Argentina	Finland	Ireland	Russian Federation
Australia	France	Italy	Singapore
Austria	Germany	Japan	South Africa
Belgium	Greece	Republic of Korea	Spain
Brazil	Gulf Co-operation Council	Luxembourg	Sweden
Canada	Hong Kong, China	Mexico	Switzerland
China	Iceland	Netherlands, Kingdom of	Turkey
Denmark	India	New Zealand	United Kingdom
European Commission		Norway	United States
		Portugal	

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

EU Legal Framework

- 3rd EU AML Directive 2005/60/EC
- Commission Directive 2006/70/EC to implement the 3rd AML Directive
- Council Decision 2000/642/JHA regulating the cooperation between FIUs
- Fund Transfers Regulation (EC) No 1781/2006
- COM(2013) 45: 4th EU AML Directive (4th AMLD)
- COM(2013) 44: new Fund Transfers Regulation

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Proposed 4th Anti-Money Laundering Directive

- Strengthening of the risk-based approach
- Stricter requirements on Customer Due Diligence/Know Your Customer
- Domestic Politically Exposed Persons
  - EP: European Commission shall draw a list accessible for competent authorities and obliged entities
- Beneficial ownership information
  - Legal persons shall transmit relevant data to a register
- Tax evasion = new predicate offence

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Two Stage Procedure

- Financial Action Task Force (FATF)
- EU legal framework
- National transposition

- State authorities
  - Financial intelligence units, supervisory authorities, law enforcement, prosecution
- Obliged entities
  - Financial and credit institutions, real estate agents, auditors, casinos etc.

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Customer Due Diligence/Know Your Customer (Counterpart)

- **Identifying** the customer and **verifying** the customer's identity on the basis of documents, data or information obtained from a reliable and independent source (**Identification**; Art. 11 (1) (a) of the 4th AMLD)
- Identify **politically exposed persons** (Art. 18 & 19 of the 4th AMLD) and **terrorists** (**Watch Lists**)
- Identifying the **beneficial owner** (**BO**; Art. 11 (1) (b) of the 4th AMLD)
- Conducting **ongoing monitoring** of the business relationship including **scrutiny of transactions** undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, the **business and risk profile** (**Transaction Monitoring**; Art. 11 (1) (d) if the 4th AMLD)
- Promptly inform the **FIU** in cases of suspicion (**Reporting**; Art. 32 (1) (a) of the 4th AMLD)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

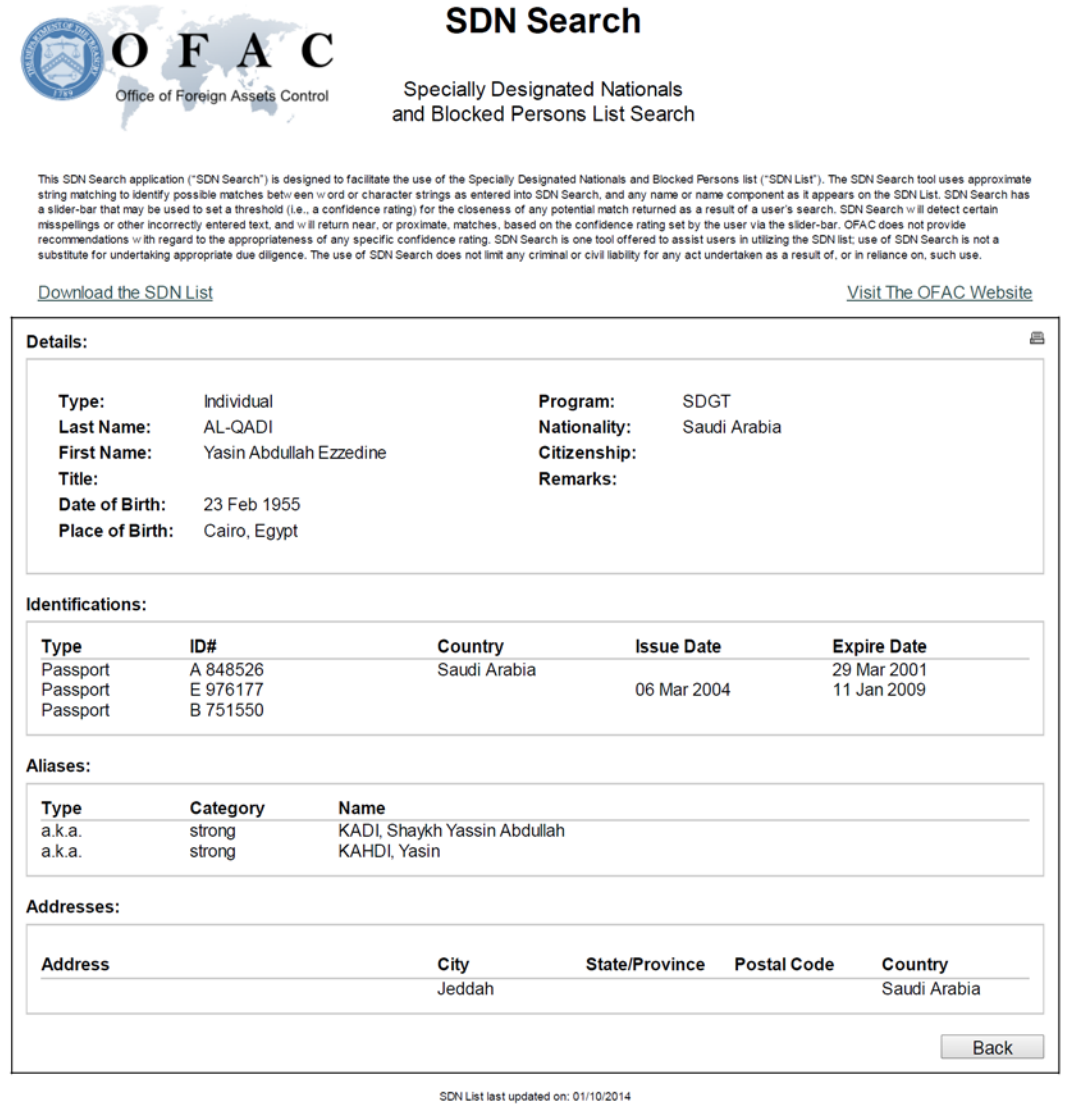
Identification

- E.g. **SironKYC** (Tonbeller AG)
- Customer acceptance questionnaire
- Automatic risk rating
  - Determines the level of necessary due diligence, to which degree new customers need to be monitored, which review and documentation obligations arise
- Interface to integrate (commercial) watch lists
  - Recognition of politically exposed persons (PEPs)
- Interface to integrate third party lists to identify BOs
  - Obtaining information about beneficial owners of companies

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Office of Foreign Assets Control (USA)



OFAC
Office of Foreign Assets Control

SDN Search

Specially Designated Nationals
and Blocked Persons List Search

This SDN Search application ("SDN Search") is designed to facilitate the use of the Specially Designated Nationals and Blocked Persons list ("SDN List"). The SDN Search tool uses approximate string matching to identify possible matches between word or character strings as entered into SDN Search, and any name or name component as it appears on the SDN List. SDN Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. SDN Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. SDN Search is one tool offered to assist users in utilizing the SDN list; use of SDN Search is not a substitute for undertaking appropriate due diligence. The use of SDN Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List Visit The OFAC Website

Details:

Type:	Individual	**Program:**	SDGT
Last Name:	AL-QADI	**Nationality:**	Saudi Arabia
First Name:	Yasin Abdullah Ezzedine	**Citizenship:**	
Title:		**Remarks:**	
Date of Birth:	23 Feb 1955		
Place of Birth:	Cairo, Egypt		

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Passport	A 848526	Saudi Arabia		29 Mar 2001
Passport	E 976177		06 Mar 2004	11 Jan 2009
Passport	B 751550			

Aliases:

Type	Category	Name
a.k.a.	strong	KADI, Shaykh Yassin Abdullah
a.k.a.	strong	KAHDI, Yasin

Addresses:

Address	City	State/Province	Postal Code	Country
	Jeddah			Saudi Arabia

Back

SDN List last updated on: 01/10/2014

RESPECT

Beneficial Owner

- FATF Recommendation 24
- **Identification of Beneficial Owner (BO)**: any natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. A percentage of 25% plus one share is considered as evidence of ownership or control (Art. 3 (5) 4th AMLD)
- Directive 2012/17/EU on the Interconnection of central, commercial and companies registers
- European Business Register (EBR)
- Bureau van Dijk
- Loyd's List
- European Business Ownership and Control Structures (EBOCS Project)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

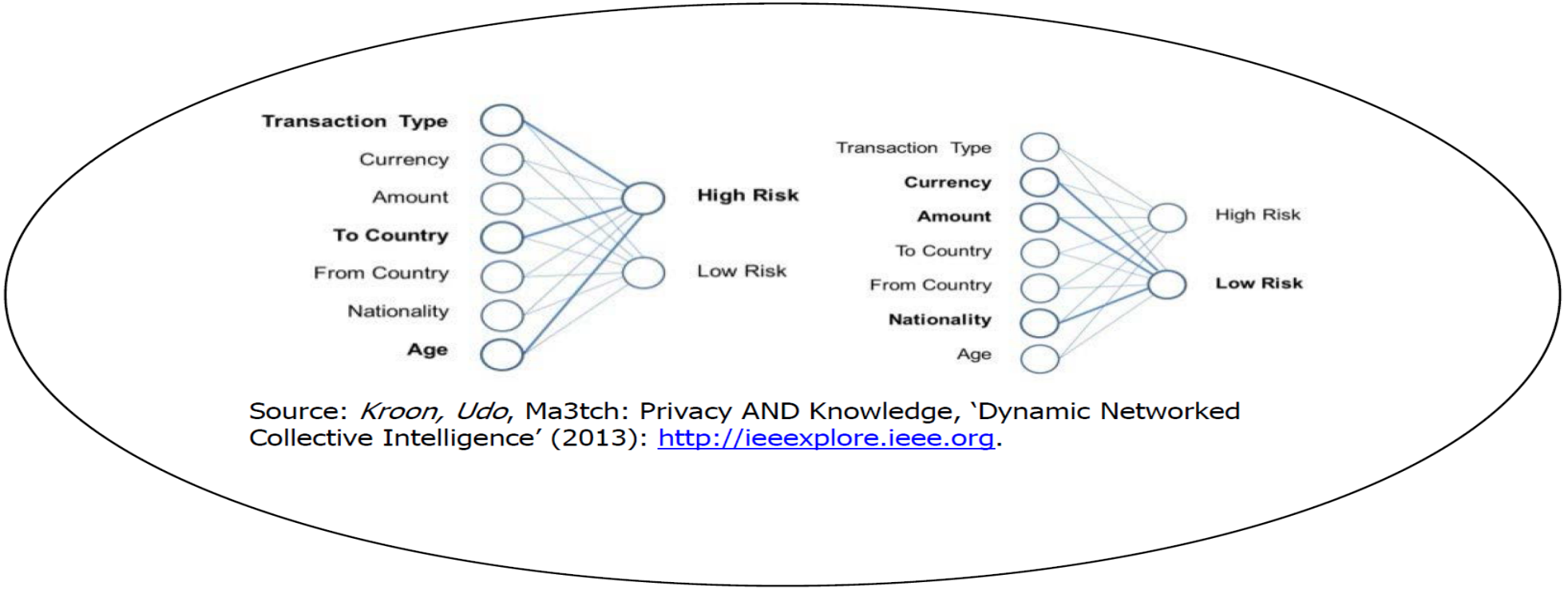
Transaction Monitoring

- Iteration of criminal activities
- Rule-based logic (rule sets)
  - IF „unrealistic business activity“ AND „large-scale cash transaction“ THEN „trigger alert“(succession of „IF“ „THEN“ conditions)
- Behaviour-based logic
- Link analyses
- Artificial intelligence

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Simplified Neural Network

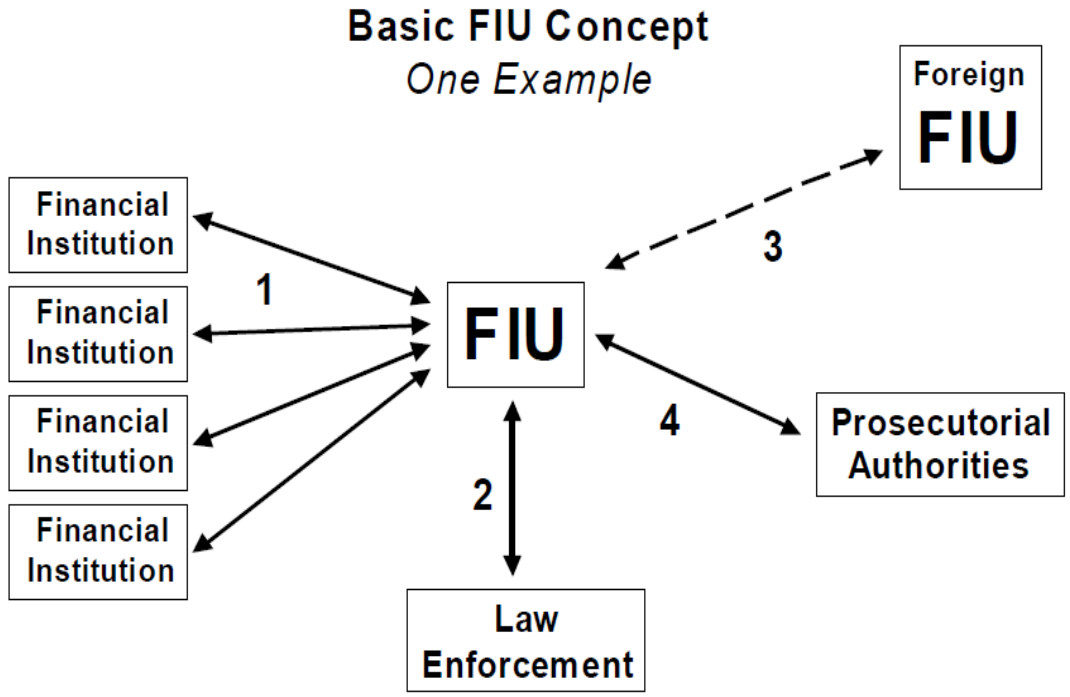


Source: *Kroon, Udo*, Ma3tch: Privacy AND Knowledge, 'Dynamic Networked Collective Intelligence' (2013): http://ieeexplore.ieee.org.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Financial Intelligence Unit

Source: *Egmont Group* (2004) Information Paper on Financial Intelligence Units and the Egmont Group, p. 1.



1. Disclosures transmitted to FIU.
2. FIU receives additional information from law enforcement.
3. Possible exchange with foreign counterpart FIU.
4. After analysis, FIU provides case to prosecutor for action.

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

FIU Co-operation

- Council Decision 2000/642/JHA
- Articles 48-54a of the 4th AMLD (as amended by EP)
- FIU.NET
- Ma³tch (Privacy by Design)
- **Spontaneously** vs. **Automatically**
  - **Automatic Exchange of Information (AEOI)**
  - Spontaneously: non-systematic communication, at any moment and without prior request
  - Automatically: systematic communication of predefined information, without prior request, at pre-established regular intervals

    (Council Directive 2011/16/EU)
- Europol‘ s Secure Information Exchange Network Application (SIENA)

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Fundamental Rights

- Monitoring Software: **Profiling**
- Watch Lists: Interference with **rights to privacy** (data protection), **property** and **freedom to travel**; **no fair trial** (ECJ case Kadi II, C-584/10 P, 18. July 2013)
- **Commercial watch lists**: no fair trial, no adequate remedy
- **PEP-lists**: no limitations, no remedy

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Conclusions (1)

- Threats to international and national security are growing …
- Surveillance is still growing BUT more and more scrutinized!
- More relaxed approach to risks required (see Breivik case)
- Case study – financial transactions: no end of surveillance in sight
  - Already extensive possibilities for data collection will increase after the new AML/CFT regime enters into force
  - List of **domestic PEPs**, **BO registries**, additional **information accompanying transfers of funds**, higher degree of **information exchange between FIUs**

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Conclusions (2)

  - AML/CFT acknowledged as **important public interest** by 4th AMLD
  - **Guidelines** and **safeguards** to limit the extent of **profiling** essential
  - **Improve** legal framework for (commercial) watch lists
- Efficiency for crime prevention has to be checked in order to respect the proportionality principle
- Legal redress is insufficiently developed

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Thank you for your attention!

Erich Schweighofer, Janos Böszörmenyi

University of Vienna

Center for Computers and Law

Vienna Centre for Legal Informatics

erich.schweighofer@univie.ac.at

janos.boeszoermenyi@univia.ac.at

http://rechtsinformatik.univie.ac.at

Jusletter IT

http://www.jusletter-it.eu

Arbeitsgruppe Rechtsinformatik
universität wien ARI
Research Centre for Computers and Law

RESPECT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

Thank you for your attention! (2)

IRIS International Conference on Legal Informatics, 26-28 February 2015

OCG KnowRight2014, Vienna, 12-14 November 2014

RESPECT Second Policy Workshop, Barcelona, 17-18 September 2014

Joint Final Event of the EU projects IRISS, RESPECT & SURVEILLE, 29-30 October 2014

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.