23C3

"KNOW YOUR CITIZEN"

Chaos Communication Congress 2006
Berlin, 27th of December 2006

Dr. Marco Gercke
Lecturer at the Faculty of Law, University of Cologne
Expert for the Council of Europe for the Convention on Cybercrime

OVERVIEW

- Overview about the current development
- No solution but basis for a discussion

OVERVIEW

- Introduction
- Control Instruments
- Motivation for stricter Control Instruments
- Example 1: “Data Retention”
- Example 2: “Encryption”

KYC

ML

- "Know your customer"
- Essential part of an anti money laundering strategy
- Obligation of financial institutions to monitor activities of their clients
- With regard to anti terrorist financing the strategy is modified to "Know your partner"
- **Intention: Detection of "suspicious transactions"**

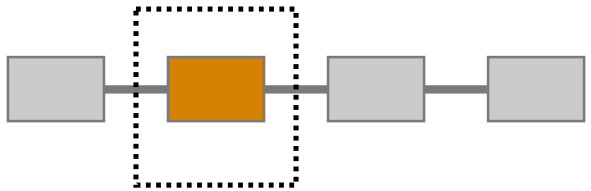
KYC

- "Know your citizen"
- Monitoring of activities / Disclosure obligations
- Similar intention: Detection of suspicious activities
  - Investigation of crimes
  - Prevention of crimes

MONITORING

- Monitoring / Surveillance is a general tendency
- Discussion about this issue is currently concentrating on the legislative approaches with regard to data retention
- Data retention is only one element in a broader strategy

ROLE OF DATA RETENT



DEVELOPMENT

- Examples

CENSUS OF POPULATION

- "Know how your citizens are living"

- Census has ever since been an important instrument for political analyses
- Question is how many information are necessary for the political purposes
- In the 1980th the German Government planed a census including **administrative penalties** for people who do not follow their obligation to return the form
- Constitutional Court in Germany limited the possibilities of census

FORM

Haushaltsbogen

Verzeichnis aller zum Haushalt gehörenden Personen:

1. Person Name	2. Person Name	3. Person Name
Vorname	Vorname	Vorname
3 Geburtsdatum Tag Monat Jahr	Tag Monat Jahr	Tag Monat Jahr
4 Geschlecht	männlich weiblich	
5 Familienstand	ledig	

REGISTRATION

CAR REGISTRATION

- "Know your citizens car"

- Car registrations obligations are a common instrument with regard to traffic control **(including administrative fee)**
- Intention is among other aspects to enable the identification of offenders in traffic related crimes **(Detection of crimes)**
- Registration identifies only the car not necessary the driver
- Identification be be circumvented (stolen car, stolen registration)

IDENTIFICATION

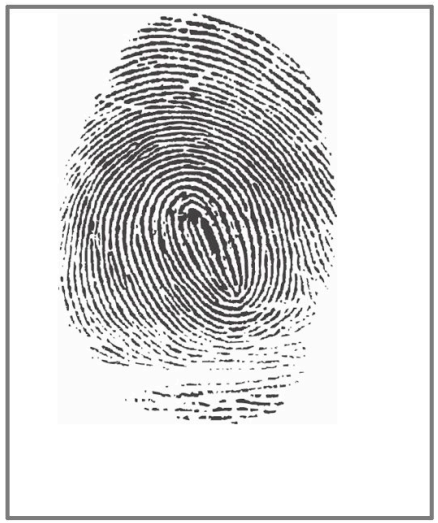
ID

- "Know where you citizens live"
- One intention is to enable law enforcement authorities to identify the regular location of a suspect **(Investigation of crimes)**
- Violation of the registration obligations goes along with **administrative penalties**
- Effectiveness of ID cards is controversially discussed

IDENTIFICATION

ID

- "Know your citizens biometric data"
- In addition to the data, that are already included further biometric data shall be included in the near future
- Among them a finger print



CCTV

- "Know what your citizens do on public places"
- Crime prevention strategy

CCTV

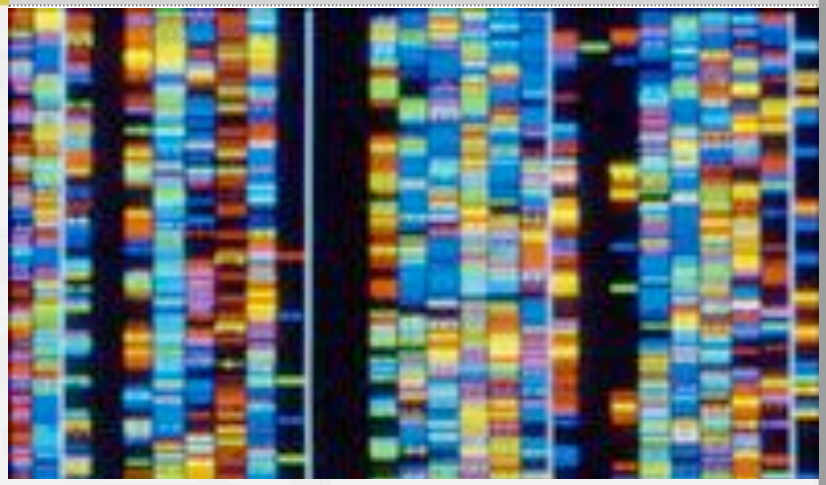
OUTLOOK

- Examples for data law enforcement authorities have no or limited access to

IDENTIFICATION

- Offenders can act without leaving finger prints
- Much more difficult to avoid leaving DNA-traces
- Information could be used to **investigate crimes**

DNA



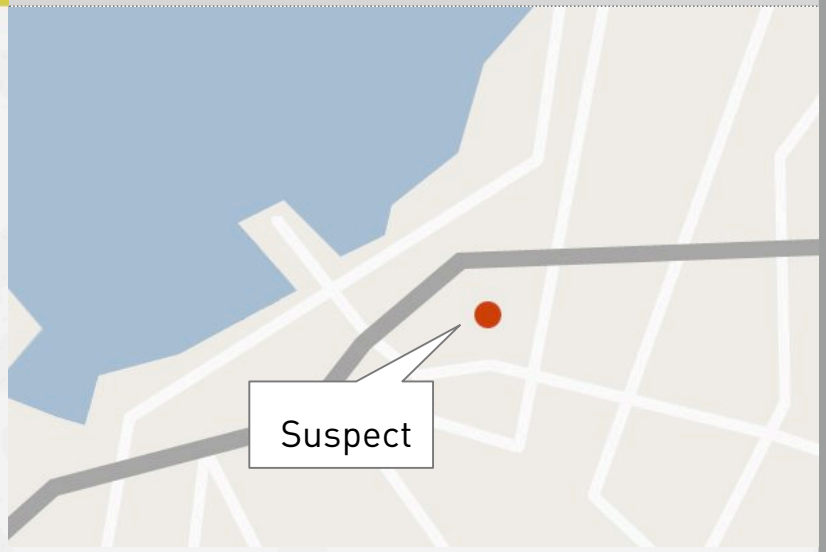
REGISTRATION

- "Know where your citizens are driving"
- Tolling System in Germany is only used for billing purposes for lorries
- Ongoing discussion about the extension of the use of the system for the detection and prevention of crimes
- Ongoing discussion about the extension of the use of the system for exact billing of car traffic
- Information could be used to **investigate crimes**

TOLL COLLECT

CELL PHONE LOCATION

- "Know where you citizens are"
- In western societies a large part of the society is using cell phones
- Phone location can be detected
- Information could be used to **investigate crimes**



PAYBACK CARDS

- "Know where you citizens are and what they consume"
- Many customers voluntarily use payback cards
- Information could be used to **investigate crimes**

PAYBACK CARD

CONTROL INSTRUMENTS

- General remarks

CONTROL INSTRUMENTS

Necessary elements

- Implementation of control instrument / Disclosure obligation
- Sanction

ADDITIONAL CONTROL

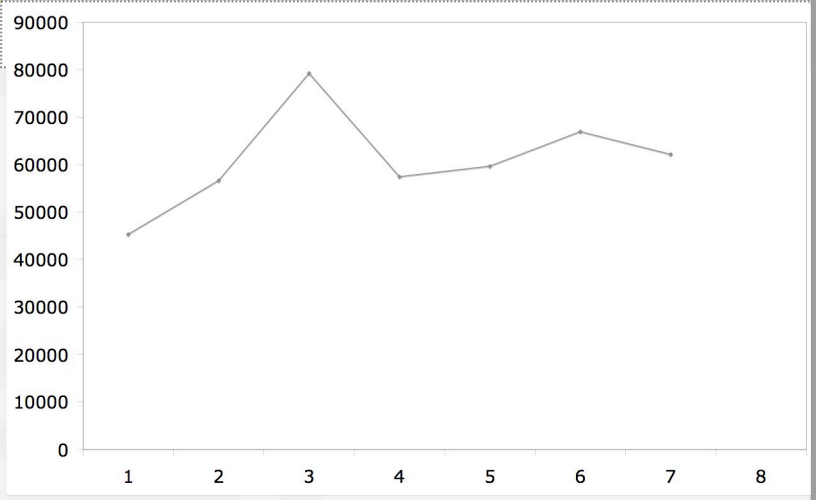
- Intensive discussion about the need for additional instruments in the fight against Cybercrime

- Motivation?

Reasons for further control instruments:

- Increasing number of Computer Crimes?
- Specific (non quantitative) reasons

COMPUTER CRIMES GERMANY



INVESTIGATION INSTRUMENTS

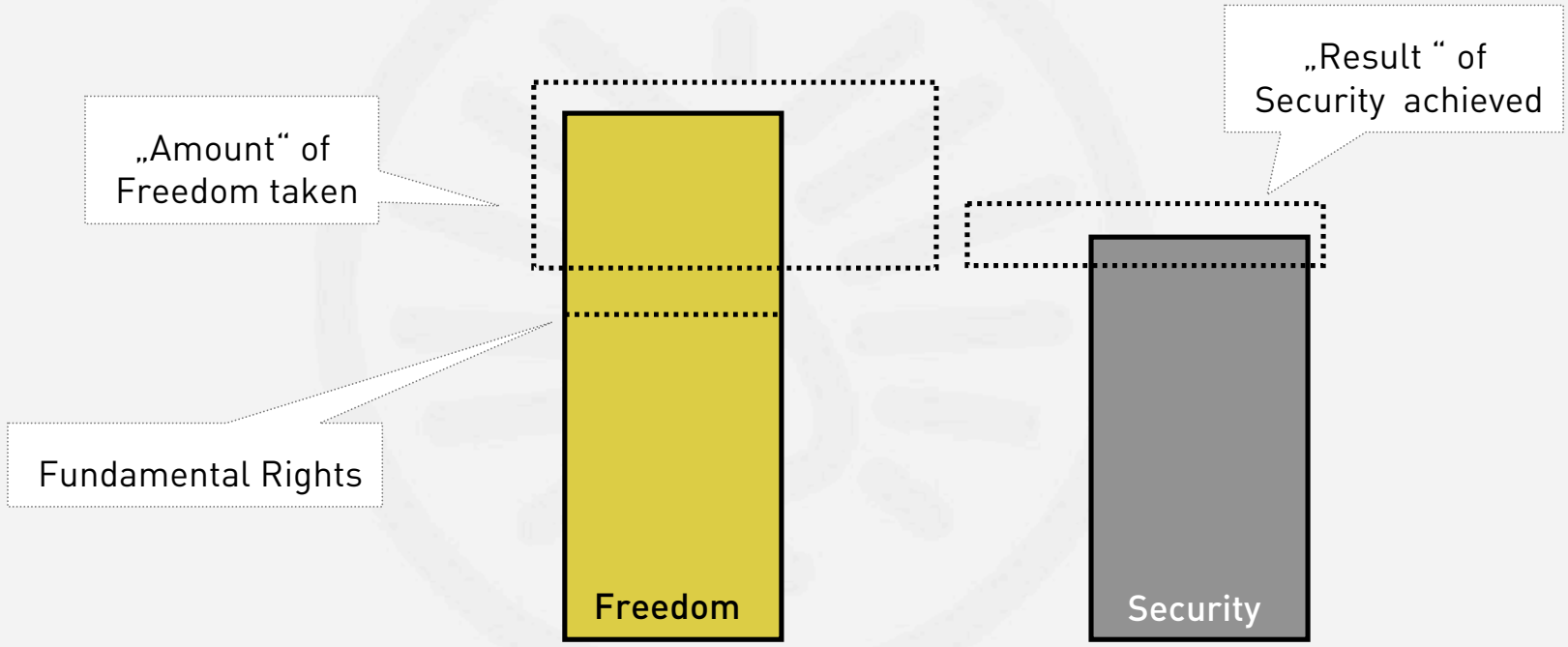
- Fight against Cybercrime goes along with a number of unique challenges for law enforcement authorities

Implementation of new investigation instruments need to be **discussed**

- Real time collection of traffic data / content data
- More effective search and seizure procedures
- Quick freeze procedures
- Smart software tools

ADJUSTMENT

- Well balanced investigation instruments are necessary



DATA RETENTION

- "Know what you citizen are doing online"

EU

- A number of initiatives for data retention legislation
- Sept. 2005 proposal for an EU-Directive dealing with data retention
- Dec. 2005 adoption by the EU Parliament
- Feb. 2006 adopted by the Council
- The key element of the Directive is the duty of Internet Providers to store certain traffic data that is necessary for the identification of criminal offenders in cyberspace

DIRECTIVE ON DATA RETENTION

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

DATA RETENTION

- Duty of retaining data needs to be implemented in the national law
- Complete change with regard to data protection law in the EU
- Providers need to provide expensive infrastructure
- Law enforcement need similar infrastructure to analyse the delivered material

Art. 3 - Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are **retained** in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

DATA PROTECTION

- Directive on privacy and electronic communications (2002/58/EC)
- Until now the EU has a very strong protection of traffic data
- Motivation: Protection of the user
- Data Retention will go along with a fundamental change

Art. 6 - Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service **must be erased or made anonymous** when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

CIRCUMVENTION

- Knowing which connection was used does not necessary gives sufficient information about the offender
  - Public Terminals
  - Wireless Lan Access Points
  - Hacked systems
  - Group of people using the computer
  - Use of certain anonymous communication devices that include components from countries without data retention legislation

OPEN WIRLESS NETWORKS

APPROACH

- The Data Retention affects all internet users
- Threat of abuse of these data
- Just the Data Retention obligation does not prevent the circumvention of the identification
- Additional laws required
- For example a ban on open wireless networks
- Registration Obligation for Public Internet Terminals (Italy)

DECREE LAW NO 144

The owner or the manager of a service where are taken place activities mentioned in the 1st paragraph are taking place is hold to observe with the purpose of monitoring the user's operation and with the purpose of archiving the above mentioned data, even if derogating from the provisions of the 1st paragraph of the art. 122 and the 3rd paragraph of the art. 123 of the Legislative Decree 30 June 2003, no. 196, as well as the measures of preventive acquisition of personal data contained in an identity document belonging to a subject that uses public locations unsupervised (that are not watched) or computer real Internet access points using the wireless technology, **have to be established in a period of 15 days** from the entrance into force of the law of conversion of the present decree, by means of a decree of the Minister of Interior, together with the Minister of Communication and the Minister for Innovation and Technologies, after consulting the Warrantor for the protection of the personal data .

ALTERNATIVE SOLUTION

- Convention on Cybercrime
- "Quick freeze" procedure
- Forcing the providers to save data that otherwise could be deleted
- No duty for general preservation of data
- No duty to hand out these protected information to the investigation authorities

Art. 16 - Expedited preservation

Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious **preservation** of specified computer data, **including traffic data**, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly **vulnerable to loss or modification**.

ENCRYPTION

- “Know your citizen’s passwords”

ENCRYPTION

- Reports about the use of encryption technology by terrorists have never been verified
- Never the less the crypto legislation is discussed
- Key Escrow is in the focus of the discussion

ENCRYPTION TECHNOLOGY (pgp.com)

UK

- Anybody encrypting documents can be forced to disclosure the key
- Refusing the order can lead to criminal sanctions
- Violation of the fundamental principle that the suspect of a crimes does not need to cooperate with the prosecution / police

REGULATION OF INVESTIGATORY POWERS ACT 2000 - Art. 53

(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.
[...]
(5) A person guilty of an offence under this section shall be liable- (a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both; (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

CONVENTION ON CYBERCRIME

- Duty to actively support the investigation
- Important investigation instrument
- Everybody apart from the suspect
- Provision is limiting the duty of access providers to protect their clients data

Art. 19 - Search Seizure

(4) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to **order any person** who has knowledge about the functioning of the computer system or **measures applied to protect** the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

ALTERNATIVE SOLUTION?

END

Thank you very much for your attention!

gercke@cybercrime.de