EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Managing privacy responsibly in the daily practices of law enforcement

Commonwealth Cybersecurity Forum

Data Protection and Privacy

London, 22-24 April 2015

Data protection at Europol

- Data processing at Europol
- Robust data protection regime
- Conditions for information exchange with partners
- Close cooperation with supervisory authorities
- Privacy by design

Cooperation partners

- Member States' competent authorities
- Non-EU States – operational partners
- Non-EU States – strategic partners
- Private sector, NGOs and academia

Key privacy challenges for law enforcement in cybercrime

- Lack of clarity on authorised interception of internet traffic
- Encryption/decryption
- Private sector data on customers
- Abuse of anonymity (Darknet, Virtual Currencies)
- Data retention
- Big data

Pseudonymisation as example of Privacy by Design

- Only exchange the information that is relevant for cooperation
- Encrypt data prior to exchange
- Cross-match encrypted data
- Prioritise among the hit results
- Exchange the hit-related, un-encrypted data between partners concerned

Why pseudonymise data?

- Risks associated with full-scale exchange of original data:
  - Due to volume
  - Due to content
- Proportionality
- Security
- Efficiency

How does it work?

- Conversion of information into sets of digits
- Specific algorythm depending on data type
- Irreversible conversion
- Relevance determined on the basis of probability of a hit
- Threshold set at < 0.000 001 that a hit occurs accidentally

Probability of algorithms per data type

Data type	Value composition	Probability
First name	2-digit value	1:100
Surname	2-digit value	1:100
Date of birth	2-digit value	1:100
Place of birth	2-digit value	1:100
Nationality	Not applicable	Not applicable
Address (street + number)	2-digit value	1:100
Postal code	2-digit value	1:100
City	2-digit value	1:100
Country	Not applicable	Not applicable
Bank account number	8-digit value	1:1,000,000
Virtual currency account	Three 2-digit values	1:1,000,000
Licence plate	2-digit value	1:100
Telephone/fax number	8-digit value	1:1,000,000
IPv4 IP-address	8-digit value	1:1,000,000
IPv6 IP-address	Three 2-digit values	1:1,000,000
Email address	Two 2-digit values	1:10,000
Nick name	2-digit value	1:100
URL	Three 2-digit values	1:1,000,000
Domain name	Three 2-digit values	1:1,000,000
Offence type	Not applicable	Not applicable
Modus operandi	Not applicable	Not applicable
Date of offence	Not applicable	Not applicable
Location of offence	Not applicable	Not applicable

Added value of the pseudynomisation model

- Accurate enough for determining relevance
- Vague enough to avoid uninvited re-engineering
- Processing can be automated to large extent
- High level of protection of personal data
- Supports the cross-matching of multiple undisclosed databases
- Probability of hit results can be adjusted
- Supports ‘fuzzy search’

Conclusions

- Sound balance between privacy and operational effectiveness
- Healthy debate with stakeholders and supervisory authorities
- Continued innovation and privacy by design
- Informed public debate on privacy versus anonymity needed
- Modernise concepts according to the digitalised reality
- Sound balance between privacy and online safety

Thank you for your attention

Olivier Burgersdijk
Head of Strategy
European Cybercrime Centre
Europol