Project on Cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version
22 November 2007
edited: 17052008

Internet-related identity theft

A discussion paper
prepared by
Marco Gercke (Germany)

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe as a contribution to the Conference "Identity fraud and theft – the logistics of organised crime", held by the Internal Security Coordinating Office of the Ministry of Interior of Portugal in Tomar, Portugal, 7-9 November 2007. It was further elaborated after that conference and is to feed into discussions on this matter at European and international levels.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

The Project on Cybercrime is funded by the Council of Europe and Microsoft.

Contents

1 Introduction

In view of the media coverage,[1] results of recent surveys,[2] as well as numerous legal and technical publications[3] in this field, it seems appropriate to speak about identity theft as a mass phenomenon.

1.1 What is identity theft?

The term identity theft – that is neither consistently defined nor consistently used – describes criminal acts where the perpetrator fraudulently obtains and uses another person's identity.[4] These acts can be carried out without the help of technical means[5] as well as online by using Internet technology.[6] Internet-related identity theft cases in particular are to a large extent based on highly sophisticated scams that demonstrate the capability of automated attacks[7] on the one hand, and show the difficulties that law enforcement agencies are faced with when investigating such offences on the other.[8] These attacks generally aim for the weakest point of the target.[9]

Examples are:

- The perpetrator persuades the victim to disclose confidential information on a website and uses it in criminal activities.[10]

---

[1] See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006 – available at: http://edition.cnn.com/2006/US/05/18/identity.theft/ (last visited: Nov. 2007); Identity Fraud, NY Times Topics – available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html (last visited: Nov. 2007); *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007 – available at: http://www.iht.com/articles/2007/03/21/business/identity.php (last visited: Nov. 2007).

[2] See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[3] See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007); *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000 – available at: http://www.privacyrights.org/ar/id_theft.htm (last visited: Nov. 2007).

[4] *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415;

[5] One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to Identity Theft see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004 – available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf (last visited Nov. 2007); *Paget*, Identity Theft – McAfee White Paper, page 6, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[6] Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report – available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf (last visited: Nov. 2007). For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007).

[7] Regarding the Challenges related to the automation see below 3.4.

[8] Regarding the Challenges for Law Enforcement Agencies see below 3.4.

[9] In cybercrime-related cases this can either be the Internet user or the user computer system he/she is using.

[10] A classic example for such scam is phishing. The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication. For details see the information offered by anti-phishing working group – available at: www.antiphishing.org (last visited: Nov. 2007); *Jakobsson*, The Human Factor in Phishing – available at:

- The perpetrator obtains credit-card information from the victim to use it for the ordering of goods and services.[11]
- The perpetrator obtains the password of the victim's email account and uses it to send out emails with illegal content.

1.2 Economic importance of identity theft

Current surveys show that identity theft is a serious challenge for societies as well as law enforcement agencies not only in terms of the number of offences, but also in terms of the losses.[12]

With regard to the reliability of such data, one should keep in mind that most statistics focus on single states and that it is uncertain if the results of the surveys are comparable to other countries. Furthermore it is uncertain to what extent users are reporting identity theft related offences.[13] Nevertheless, statistics indicate trends and the scope of the problem. Recent surveys and analysis assume for example that:

- In the United Kingdom, the cost of identity theft to the British economy was calculated at £1.3 billion every year.[14]
- Estimates of losses caused by identity theft in Australia vary from less than US$1 billion to more than US$3 billion per year.[15]
- The 2006 Identity Fraud Survey estimates the losses in the US at US$56.6 billion in 2005.[16]

---

http://www.informatics.indiana.edu/markus/papers/aci.pdf (last visited: Nov. 2007); *Gercke*, Criminal Liability for Identity Theft and Phishing, CR 2005, 606.

[11] Identity Theft related to Credit Card Fraud remains the most common combination. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

[12] See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[13] This problem is not limited to surveys but also important for law enforcement agencies. Experts involved in the fight against cybercrime do on a regular basis encourage victims of cybercrime to report to local authorities. "The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, - available at: http://www.heise-security.co.uk/news/80152 (last visited: Nov. 2007).

[14] See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf (last visited: Nov. 2007).

[15] *Paget*, Identity Theft – McAfee White Paper, page 10, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[16] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report – available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf (last visited: Nov. 2007).

1.3 Scope of the discussion paper

The objective of the discussion paper is to identify and review legal approaches to criminalise internet-related identity theft. In order to evaluate the need for a harmonisation of identity theft legislation as well as possible legislative solutions, the present paper takes two approaches:

- It first of all analyses the most common internet-related offences with the aim to identify common principles of all offences. The identification of common principles is necessary to describe the elements of a provision (e.g. acts and results covered by the provision) designed to criminalise identity theft.
- In addition the paper analyses existing criminal law provisions to evaluate how far they already cover identity theft related offences. The discussion paper will in this context focus on the US approach in 18 U.S.C. § 1028 / 18 U.S.C. § 1028 and the Convention on Cybercrime – that is currently the only existing international Convention that provides a comprehensive legal framework in the fight against Cybercrime.[17]

This question is moving higher on the political agenda in Europe. For example, the European Commission stated in a recent communication that identity theft is not yet criminalised in all EU member states.[18] In this context the Commission proposed "that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States" and announced that it would shortly commence consultations to assess if legislation was appropriate.[19]

[17] For more information related to the Convention on Cybercrime see: *Gercke*, The slow Wake of a global approach against cybercrime, CRi 2006, page 150 et seqq.

[18] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267.

[19] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267.

2 Difficulties in the fight against identity theft

2.1 Impact of the identity architecture

The fact that identity theft has become one of the most widespread cybercrimes is related to the vulnerability of the identification architecture. These vulnerabilities are not created by the perpetrators that commit the crime, but exploited by them.[20] Criticism regarding this vulnerability particularly concerns single identification data that are not protected by sufficiently secure systems. One example is the Social Security Number (SSN) in the United States.[21] The SSN was created to keep an accurate record of earnings.[22] Due to this aim, no security regime was developed to ensure that the use of the SSN in identification processes would not involve security risks. Contrary to its original intentions, the SSN is today widely used for identification purposes.[23] And as it is insufficiently protected, perpetrators are able to cause great harm (e.g. by gaining access to a person's existing accounts, applying for credit in the victim's name and obtaining even more information about the victim for further use) solely based on the SSN.[24]

2.2 Availability of information

Two developments are responsible for the increasing amount of publicly available identity-related information. Currently a number of highly successful Internet services like "facebook"[25], "MySpace"[26] and "Second Life"[27] are based on the principle of developing a culture of digital identities. Users assigned to such services transfer a part of their social activities to the Internet. This process often involves the disclosure of private information which can be abused by perpetrators. Due to the fact that the majority of Internet users use a limited number of very popular services, as well as the availability of search engines that are specialised in the detection of private information about a person,[28] it is rather easy for a perpetrator to collect that information and use it for criminal purposes.[29]

The second development is closely related to the transfer process. As highlighted previously, the information that is often made publicly available cannot in general be used on its own, but only in combination with other data in order to take over the identity of another person. The perpetrators are therefore highly interested in linking different identity-related information. In this they are – indirectly – supported by the current global trend trends in

[20] *Solove*, The legal construction of Identity Theft, page 4, Symposium: Digital Cops in a virtual environment Yale Law School (March 26-28, 2004).

[21] *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000 – available at: http://www.privacyrights.org/ar/id_theft.htm (last visited: Nov. 2007).

[22] *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[23] *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34.

[24] Regarding the risks related to the SSN see: *Solove*, The legal construction of Identity Theft, page 3, Symposium: Digital Cops in a virtual environment Yale Law School (March 26-28, 2004).

[25] www.facebook.com

[26] www.myspace.com

[27] www.secondlife.com

[28] See for example www.spock.com.

[29] Having access to true identity-related information can be from great interest of the offender even if these information do not enable him to act by using this identity. The offender can especially use the information to improve synthetic identities by mixing generated data with existing data. Regarding the importance of synthetic identities in identity theft scams see: ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (last visited: Nov. 2007).

the e-business to link digital identities.[30] Data mining systems are used for example to analyse the behaviour of customers; they even try to predict their future behaviour based on an analysis of consumer-related data collected in various databases. A recently published study highlights the threats of this process for society as well as for the individual.[31] If the perpetrators manage to improve their skills in linking digital identities, they can commit offences by using the identity of another person without referring to illegal means, while obtaining the identity-related information.

2.3 Missing identity verification procedures

The popularity of digital identities and the related process of transferring parts of one's social life to the Internet are combined with the problem that the instruments that were developed to identify and prevent perpetrators from abusing other people's identity do not in general apply in the digital world.[32] Many of these instruments are based on the personal contact of the people acting. Checking tangible identifying documents or physical recognitions (especially between individuals who previously established a relationship) is easy in the real world but difficult in the digital world.[33] The development of effective identification instruments that can be used on the Internet has just started.[34]

2.4 Investigation-related challenges for law enforcement agencies

When investigating internet-related identity theft, law enforcement agencies are faced with a number of challenges comparable to those regarding other cybercrimes, but not necessarily comparable to more traditional investigations. Some of the most important challenges are:

- **Potential number of victims**

  There seem to be more than 1 billion Internet users worldwide.[35] This number is expected to increase continuously in the coming years.[36] With this the number of potential victims of identity theft increases.

- **Availability of instructions on how to carry out an offence**

  It is not just identity-related information that perpetrators can find on the Internet. Reports highlight the risks that go along with the legal use of search engines for illegal

---

[30] See: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available online at: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (last visited: Nov. 2007).

[31] *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available online at: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (last visited: Nov. 2007).

[32] Similar difficulties with regard to the switch to virtual currencies as classic AML approaches are difficult to implement with regard to virtual currencies. Regarding virtual currencies see: *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

[33] *Paget*, Identity Theft – McAfee White Paper, page 4, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[34] Technology that enables the verification of the user is not only relevant in order to avoid or detect identity theft but also with regard to the protection of minors from having access to potentially harmful content. Regarding technical approaches for age verification systems see: See *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150 - available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[35] According to "Internet World Stats" more than1,15 Billion people are using the Internet by 2007 (the statistic are available at: http://www.internetworldstats.com/stats.htm) (last visited: Nov. 2007).

[36] The greatest potential for further growth have developing countries. In 2005 the number of Internet users in developing countries surpassed the number of users in developed countries. See: Development Gateway's Special Report, Information Society – Next Steps?, 2005 – available at: http://topics.developmentgateway.org/special/informationsociety (last visited: Nov. 2007).

purposes.[37] A perpetrator who plans an attack can find detailed information on the Internet that explains how to build a bomb by using chemicals that are available in regular supermarkets.[38] With regard to identity theft, instructions, including information on how to obtain and create an identity, are available on various websites.[39]

- **International dimension**

Similarly to other cybercrimes, identity theft offences often have an international dimension. If the perpetrator and the victim are not based in the same country then the investigation requires the co-operation of law enforcement agencies in all countries that are involved.[40] The principle of national sovereignty does not in general allow one country to carry out investigations within the territory of another country without permission from the local authorities.[41] The related formal requirements and especially the average time that is necessary to respond to requests from foreign law enforcement agencies often hinder the investigations.[42]

- **Automation**

One of the greatest advantages of information technologies is the possibility to automate certain processes, and perpetrators make use of this potential. One of the most notorious examples is spam.[43] The abuse of email services to send out unsolicited bulk messages is based on the automation of the sending process.[44] Without that it would not be possible to deliver millions of emails within a rather short period of time.[45] The same technology is used in email-based "phishing" scams.

---

[37] See *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004 – available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[38] An example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

[39] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 10, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007).

[40] Regarding the need for international cooperation in the fight against cybercrime see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seqq. – available at: http://media.hoover.org/documents/0817999825_35.pdf; (last visited: Nov. 2007). Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seqq. – available at: http://media.hoover.org/documents/0817999825_1.pdf (last visited: Nov. 2007).

[41] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1 – available at: http://www.law.uga.edu/intl/roth.pdf. (last visited: Nov. 2007).

[42] See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, CRi 2006, 142. For examples see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension - in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16 – available at: http://media.hoover.org/documents/0817999825_1.pdf (last visited: Nov. 2007).

[43] The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition see: ITU Survey on Anti-Spam legislation worldwide 2005 -, page 5 – available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf (last visited: Nov. 2007).

[44] For more details on the automation process regarding spam mails and the related challenges for law enforcement agencies see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21 – available at: http://www.michbar.org/journal/pdf/pdf4article1163.pdf. (last visited: Nov. 2007).

[45] Today e-mail provider and organizations report that up to 85% of all e-mails are spam. See for example: The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 percent of all e-mails are spam. See http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf (last visited: Nov. 2007). The provider postini published a report in 2007 that identifies up to 75 percent spam e-mail – see http://www.postini.com/stats/. The Spam-Filter-Review identifies up to 40% spam e-mails – see http://spam-filter-review.toptenreviews.com/spam-statistics.html. (last visited: Nov. 2007).

3 Common principles - a prerequisite for drafting identity theft legislation

As pointed out previously, drafting legislation to criminalise identity theft requires the description of covered acts. The identification of common principles is therefore a necessary preparation for the definition of the elements of a criminal law provision (e.g. acts and results covered by the provision) designed to criminalise identity theft. Summarising the huge variety of offences related to identity theft in a single provision requires the identification of constitutive elements of all relevant scams.

3.1 Defining "identity theft"

The first question is therefore whether common principles can be extracted from the standard definitions used to describe the underlying offence. A clear definition of the phenomenon could therefore be the basis for the development of legal solutions. Such a clear definition of the term "identity theft" is currently missing.[46] One of the many general approaches is the following:

> "Identity theft" may be used to describe the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive.[47]

While this definition focuses on the act of obtaining the identity, other definitions and descriptions of the phenomenon identity theft include the purpose of obtaining the data or even clear requirements regarding the subsequent acts.[48]

The main difficulty related to the definition is the inconsistent use of the term. Its use varies in different countries. While most US publications use the term "identity theft", the term "identity fraud" is very popular in the UK.[49] Other terms used are for example "phishing", "account takeover" or "account hijacking".[50] Some use the term to describe any act of obtaining elements of an identity, while others only use it to describe the use of another person's identity in relation with other offences.

3.1.1 Use of the term "identity theft" in surveys and publications

The different ways the term identity theft is used can be demonstrated by referring to three publications in this area:

- The 'Consumer Fraud and Identity Theft Complaint Data' survey published by the US Federal Trade Commissions points out that: "Credit card fraud (26%) was the most common form of reported identity theft".[51]

---

[46] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 22 – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

[47] *Paget*, Identity Theft – McAfee White Paper, page 5, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[48] See below 2.1.

[49] Regarding the different country specific approaches in the definition see *Paget*, Identity Theft – McAfee White Paper, page 15, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007); *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 22. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

[50] As pointed out previously even those publications that use the term "Identity Theft" do not use it consistently.

[51] Consumer Fraud and Identity Theft Complaint Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

The report links the act of obtaining identity-related information ("theft") to the criminal offence that is committed by using this information (in this case fraud committed by using credit card information).

- The report 'Identity Theft: Do You Know the Signs?' of the Fraud Advisory Panel lists certain forms of identity theft. One example given in the report is the following:

> The fraudster will obtain a certified copy of the victim's birth certificate (which is both straightforward and lawful) and apply for identification documents on the basis of that birth certificate. Identification documents could include passports, driving licences and national insurance.[52]

In this example of identity theft there is again a link between the act of obtaining the information and further action – but unlike in the previous example the second act is not related to fraud but to the use of traditional identification documents.

- The report 'Combating Identity Theft – A Strategic Plan', published by the US President's identity theft Task Force,[53] lists, among other issues, statutes criminalising identity theft. Among the "Computer-related identity theft Statutes" the report mentions 18 U.S.C. § 1030(a)(5) – a provision that criminalises certain acts aiming at the integrity and availability of computer systems and data.[54] Hindering a computer system from functioning or deleting files is not directly related to obtaining confidential information but to related offences that might be committed if the perpetrator is using malicious software that affects the integrity of the victim's computer system.[55]

---

[52] See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf (last visited: Nov. 2007).

[53] Combating Identity Theft – A Strategic Plan, US President's Identity Theft Task Force, page 66, 2007 – available at: http://www.idtheft.gov/ (last visited: Nov. 2007).

[54] *§ 1030. Fraud and related activity in connection with computers*

Whoever—

[...]

(5) (A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

[...]

[55] See below 5.3.

3.1.2 Use of the term "identity theft" in existing legislation

Only a few states have criminal law provisions in place that explicitly aim at a criminalisation of identity theft and define or precisely describe the term.[56] The most well-known approaches of defining identity theft were undertaken in the USA.

- One example is 18 U.S.C. § 1028(a)(7), that defines identity theft as:

  > knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

  The provision covers a wider range of acts related to means of identification. Unlike the way the term identity theft is used in the Consumer Fraud and Identity Theft Complaint Data survey, it is especially not mandatory with regard to § 1028(a)(7) that the act is related to fraud.

- Another description is provided by the US Federal Trade Commission. 15 U.S.C. 1681a(q)(3) contains a brief description of the term "identity theft":

  > Identity theft - the term "identity theft" means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.

  The main difference to the description provided by 18 U.S.C. § 1028(a)(7) is the fact that 15 U.S.C. 1681a(q)(3) links the term identity theft to fraud. This limits the application of the provision in other cases where the offender is using the identity-related information for other offences. In addition, the provision covers the use of the information but not the act of obtaining it.

- Based on 15 U.S.C. 1681a(q)(3), the Federal Trade Commission provided a more detailed description of identity theft: [57]

  > (a) The term 'identity theft' means a fraud committed or attempted using the identifying information of another person without lawful authority.
  >
  > (b) The term 'identifying information' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any
  >
  > (1) Name, Social Security number, date of birth, official state- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.
  >
  > (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.
  >
  > (3) Unique electronic identification number, address, or routing code.
  >
  > (4) Telecommunication identifying information or access device.

  Like 15 U.S.C. 1681a(q)(3), the description links the term identity theft to fraud and only covers the act of using the identity-related information.

3.1.3 Provisional result

---

[56] For an overview about identity theft legislation in Europe see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 et. seqq. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf (last visited: Nov. 2007); Legislative Approaches To Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007.

[57] Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, Federal Register 69, no. 82.

The overview shows that no standard definition for identity theft exists. Some definitions focus on the act of obtaining the information.[58] Drafting criminal law provisions on the basis of such a definition would make Internet-related identity theft a particular case of data espionage.[59] Based on the assumption that adequate cybercrime legislation is in place, implementing a specific provision criminalising the act of identity theft would not be necessary for prosecuting Internet-related identity theft offences. The function of an additional provision would therefore be limited to a clarification or aggravation of the sentence.

A similar inconsistency can be identified with regard to the offences that the act is related to. While some definitions make a mandatory link between identity theft and fraud,[60] others cover any use of the information for criminal purposes. What all these subsequent offences that follow the identity theft have in common is that they are already criminalised. Depending on what kind of offence is committed, identity theft is therefore again only a particular case of this offence and – if adequate cybercrime legislation is already in place – the implementation of a specific provision is not mandatory to allow prosecution.

While focusing on the above-mentioned examples of the inconsistency of definitions, with regard to the acts covered (that is, obtaining information or using information), the offences appear to be only a particular case of well known offences that are already criminalised in many countries. This is at least the case with regard to Internet-related offences that are the focus of this discussion paper. One of the few fundamentally different approaches is 18 U.S.C. § 1028(a)(7). Based on this provision, law enforcement agencies are able to prosecute an offender even if he neither obtained the identity-related information nor used them for criminal purposes. The criminalisation only requires some sort of interaction ("transfer, possession, use") with such information with the intention to commit, aid or abet an offence. As a result, the pure possession of data intended to be used later on for criminal offences is already criminalised. This approach goes beyond the cybercrime legislation of most countries.[61]

The only consistent element of the identity theft definitions is therefore the fact that the conduct is related to one or more of the following phases:

- Act of obtaining identity-related information;
- Act of possessing or transferring the identity-related information;
- Act of using the identity-related information for criminal purposes.

This conclusion has a significant impact on the development of legislative approaches against identity theft. Identifying a structure of the underlying acts is an essential

[58] See above 4.1.

[59] If the offender is obtaining non-identity-related information by using means of electronic communication provisions criminalising data espionage or illegal access do in general cover the act. There are two different approaches in criminalising data espionage. Some countries follow a narrow approach and criminalise data espionage only if specific secret information are obtained. An example is § 1831 USC that criminalised economic espionage. The provision does not only cover data espionage but other forms of obtaining secret information as well. Other countries followed a broader approach and criminalise the act of obtaining stored computer data even if they do not contain economic secrets. An example is the previous version of § 202a German Penal Code.

[60] See for example 15 U.S.C. 1681a(q)(3).

[61] Regarding the identity theft legislation in the US, The Netherlands, Great Britain, France and Belgium see: *Vries/Tgchelaar/Linden/Hol*, Identiteitsfraude: End Afbakening, 2007.

requirement for a single-provision based approach criminalising a certain conduct. The fact that the majority of identity theft offences have nothing more in common than their relation to one or more of the three phases makes it difficult to address the offence by a single provision.

With regard to the inconsistency in use, it is necessary to change the focus from analysing existing provisions and definitions to analysing fundamental principles of the most important identity theft scams.

3.2 Methods, targets and motivation

The following chapter analyses three elements of the most popular identity theft scams: the methods used, the targets of the attacks and the motivation of the perpetrator.

3.2.1 Overview of the methods used to obtain identity-related data

The following overview gives a summary of the most important techniques used to obtain identity-related information. This is important for the development of a systematic approach for defining essential elements related to the act of obtaining the identity-related information.

- **Physical methods**

  Examples of physical methods are stealing computer storage devices with identity-related data, searching trash ("dumpster diving"[62]) or mail theft.[63] The 2007 CSI Computer Crime and Security Survey[64] shows that nearly 15% of the losses of respondents with regard to computer-related offences were related to the theft of confidential data and mobile hardware.[65] Although it is questionable if the theft of computer hardware is considered to be a computer-related offence, the statistic underlines the importance of physical methods to obtain identity-related data.[66]

- **Search engines**

  Examples of search approaches are the use of search engines or file-sharing systems to identify and obtain identity-related data. Search engines enable users to search millions of web pages within seconds. This technology is not only used for legitimate purposes. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues, as well as personal information that can be used in identity theft scams. One aim of the perpetrator can be for example to search for insecure password protection

---

[62] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004 – available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf (last visited Nov. 2007); *Paget*, Identity Theft – McAfee White Paper, page 6, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[63] This method is not cosidered as an Internet-related approach.

[64] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of Cybercrime businesses. It is based on the responses of 494 computer security practitioners from in U.S corporations, government agencies and financial institutions. The Survey is available at: available at: http://www.gocsi.com/ (last visited: Nov. 2007).

[65] CSI Computer Crime and Security Survey 2007, page 15 – available at: http://www.gocsi.com/ (last visited: Nov. 2007).

[66] Regarding the definition of computer crimes and cybercrime see: *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18 – available at: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

systems in order to obtain data from this system.[67] Reports highlight the risks that can go along with the legal use of search engines for illegal purposes.[68]

Further risks related to the availability of identity-related information are file-sharing systems. The legal discussion about file-sharing systems is dominated by copyright issues. Nevertheless, the US Congress recently discussed the possibilities of file-sharing systems to obtain personal information that can be abused for identity theft.[69] It was highlighted that the file-sharing software can not only be used to search for music and video files stored on the computer of other users of the file-sharing network, but also for private information.

- **Insider attacks**

  Insiders, who have access to stored identity-related information, can use their access to obtain that information. The 2007 CSI Computer Crime and Security Survey[70] shows that more than 35% of the respondents attribute more than 20% of their organisation's losses to insiders. The results of the survey correspond with reports about employees obtaining thousands of credit reports and credit card information.[71]

- **Attacks from the outside**

  Apart from attacks from the inside, perpetrators can hack into computer systems to obtain data. The offence that is often described by the term "hacking" criminalises the unlawful access to a computer system.[72] It can involve malicious software like sypware or keylogger.[73] Some of the most well-known victims of hacking attacks are NASA, U.S. Air Force, the Pentagon, Yahoo, Google, Ebay, the Estonian Government and the German Government.[74] Reports about hackers that successfully broke into computer systems to obtain millions of credit card information illustrate the scope of the risk.

- **Social engineering regarding the disclosure of identity-related information**

  Perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective

---

[67] For more information see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[68] See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004 – available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[69] See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007 – available at: http://oversight.house.gov/documents/20071017134802.pdf (last visited: Nov. 2007).

[70] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of Cybercrime businesses. It is based on the responses of 494 computer security practitioners from in U.S corporations, government agencies and financial institutions. The Survey is available at: available at: http://www.gocsi.com/ (last visited: Nov. 2007).

[71] The 2005 Identity Theft: Managing the Risk report is taking regard to an incident where an employee of a US company that supplied banks with credit reports used confidential computer passwords to access and download the credit reports of over 30,000 consumers during a three year period. See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2 – available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf (last visited: Nov. 2007).

[72] In the early years of the development of computers the term hacking was used in a different way. It described the attempt to get more out of a system (software or hardware) than it was designed for. Within this context the term described a constructive activity.

[73] For an overview about the tools used see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention – available at: http://www.212cafe.com/download/e-book/A.pdf.

[74] For an overview of victims of hacking attacks see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

scams to obtain secret information (e.g. bank account information and credit card data) by manipulating users through social engineering techniques.[75] "Phishing" has recently become one of the most important crimes related to cyberspace.[76] The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords by impersonating a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.[77]

3.2.2 Overview of the data that perpetrators attempt to obtain

As highlighted previously, it is in general not the identity as a whole but selected identity-related data that the perpetrators are attempting to obtain in cybercrime-related identity theft cases. The type of data that the perpetrators target varies, but unlike in individually designed attacks, the approaches to obtain data by automated attacks (like for example in phishing or spyware attacks) are targeting common data. Examples are:

- **Social Security Number (SSN) and passport numbers**

  The SSN that is used in the USA is a classical example of a single identity-related data that perpetrators are aiming for. Although the SSN was created to keep an accurate record of earnings, it is currently widely used for identification purposes.[78] The perpetrators can use the SSN as well as obtained passport information to open financial accounts, take over existing financial accounts, establish credit or run up debt.[79] If the perpetrator succeeds in infecting a computer system with malicious software he can use the software to search all available files on the hard disk for documents containing numbers that show characteristics of a SSN and transfer them from the victim's computer.

- **Date of birth, address and phone numbers**

  The above mentioned identity-related information is classic data that can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN).[80] Having access to that additional information can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently available on a large scale on the Internet – either published voluntarily in one of the various identity-related fora,[81] or based on legal requirements as imprint on

---

[75] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001 – available at: http://www.securityfocus.com/infocus/1527.

[76] See the information offered by anti-phishing working group – available at: www.antiphishing.org (last visited: Nov. 2007).

[77] *Jakobsson*, The Human Factor in Phishing – available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf (last visited: Nov. 2007); *Gercke*, Criminal Liability for Identity Theft and Phishing, CR 2005, 606; *Paget*, Identity Theft – McAfee White Paper, page 4, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[78] *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[79] See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000 – available at: http://www.privacyrights.org/ar/id_theft.htm (last visited: Nov. 2007).

[80] *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000 – available at: http://www.privacyrights.org/ar/id_theft.htm (last visited: Nov. 2007).

[81] Examples is the online community Facebook (www.facebook.com).

websites.[82]

- **Passwords for non-financial accounts**

  Having access to passwords for accounts enables perpetrators to change the settings of the account and use it for their own purposes.[83] They can for example take over an email account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods. User names and passwords can for example be obtained by intercepting unencrypted wireless communication.

- **Financial account information**

  Like the SSN, information regarding financial accounts is a popular target for identity theft. This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes. Similar to the SSN, credit card numbers in particular can be rather easily identified by performing search procedures on the victim's computer.

3.2.3 Overview of the motivation of the perpetrator

The motivation of the perpetrators varies as much as the methods they use, as pointed out previously. Given that obtaining the information is in general the only necessary "preparation" of the act carried out by using the information, the motivation is very much determined by this second phase.

- **Requirement of further acts (economic crimes)**

  In most cases the access to identity-related data enables the perpetrator to commit further crimes.[84] The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. An example is computer-related fraud.[85]

- **Sell the information**

  Another approach is to sell the data[86] which can then be used by other perpetrators. Credit card records are for example sold for up to US$60.[87] In this context the motivation of the perpetrator is to generate direct profit without carrying out the offence for which the obtained data are required.

- **Hiding the identity**

---

[82] See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce):

[83] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004 – available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf (last visited Nov. 2007);

[84] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

[85] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

[86] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007).

[87] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2 – available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf (last visited: Nov. 2007).

Perpetrators can use the data they obtained to hide their real identity. An example is the use of hijacked email accounts to send out messages with illegal content. In this context it is important to point out that despite the fact that such use of data in phase 2 might not be a criminal offence, it can involve serious harm for the victim.[88]

3.2.4 Provisional result

The overview shows that in none of the three analysed areas do common principles exist. The ways in which identity-related information is obtained varies. Email phishing scams show that it is not even necessary for perpetrators to circumvent protection mechanisms and then search for the information. Many highly successful phishing scams are based on the disclosure of information by the victim. The types of data that perpetrators aim for show a similar diversity. They range from information like the Social Security Number, to the address of the victim that – without connection to other data – has very little potential for causing great losses. Not even the motivation of the perpetrators is consistent. While some perpetrators intend to use the data for their own criminal activities, others are planning to sell the information or use it for acts that are not covered by the traditional criminal law.

The only consistent element of the offences is again[89] the fact that the condemned behaviour is related to one or more of the following phases:

- Act of obtaining identity-related information;
- Act of possessing or transferring the identity-related information;
- Act of using the identity-related information for criminal purposes.

As pointed out before, this conclusion has a significant impact on the development of legislative approaches in the fight against identity theft. Identifying a structure of the underlying acts is an essential requirement for a single-provision based approach to criminalise certain conduct. The fact that the majority of identity theft offences have nothing more in common than the fact that they can be split in two phases makes it difficult to address the offence with a single provision.

3.3 Extracting common principles

Taking into account the above mentioned inconsistency, as well as the consistency with regard to the phases, two common elements can be extracted:

3.3.1 Identity

It is necessary to distinguish the sociological and philosophical term "identity" – that is used to describe the sum of elements that are creating an identity of a person – and the target of "identity theft". As pointed out by the definition of "identifying information" in 15 U.S.C. 1681a(q)(3), it is not necessarily the whole identity that is abused by the perpetrator. Some digital data, such as passwords, account names and login information may not be considered elements of a person's legal identity, but with regard to the fact that such data can be "identifying" and provide access to other

[88] *Paget*, Identity Theft – McAfee White Paper, page 11, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[89] See above 4.1.

private data. This is especially relevant for countries where single data (like passport number, tax number, social security number) are used for identification purposes. With regard to the importance of those identity-related data, it is necessary to evaluate their relevance if an approach to address identity theft by the means of criminal law is intended. [90]

Apart from the fact that the target of the offender is not necessarily the whole identity, it is important to highlight that the term "identity theft" is not only used in relation to existing identities but also if the offenders are using synthetic identities.[91] A report published by ID Analytics in February 2007 shows that in the majority of fraud-related cases of identity theft the offenders did not use true-name identities but synthetic identities.[92] Based on the results of the study, less than 15% of all cases involved true-name identities.[93] Synthetic identities can either be based solely on generated data or combine generated and real identity related data.[94]

Taking the above mentioned aspects into consideration demonstrates the difficulties in defining common principles with regard to the identity-related data. It is particularly uncertain whether it will be possible to cover solely generated information and real identity related information with a single provision.

3.3.2 Acts covered

The term identity theft is not used consistently. It is first of all used to describe the act of obtaining the identity of another person ("theft"). In addition the term is used to describe the possession and use of the act. Finally the term is used to describe offences carried out by using another person's identity.[95] The fact that very often the subsequent offence is related to fraud explains the popularity of the term "identity fraud".

If the harmonisation of identity theft legislation in the EU is intended, it is necessary to evaluate the need for criminal law provisions related to all three phases[96]:

- First of all the act of obtaining identity-related information (Phase 1). This part of the offence can for example be carried out by using malicious software or phishing attacks.

---

[90] *Paget*, Identity Theft – McAfee White Paper, page 4, 2007 – available at: http://www.mcafee.com/us/threat_center/white_paper.html (last visited: Nov. 2007).

[91] Regarding synthetic identities related identity theft scams see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007 – available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1

[92] See ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (last visited: Nov. 2007).

[93] See ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (last visited: Nov. 2007).

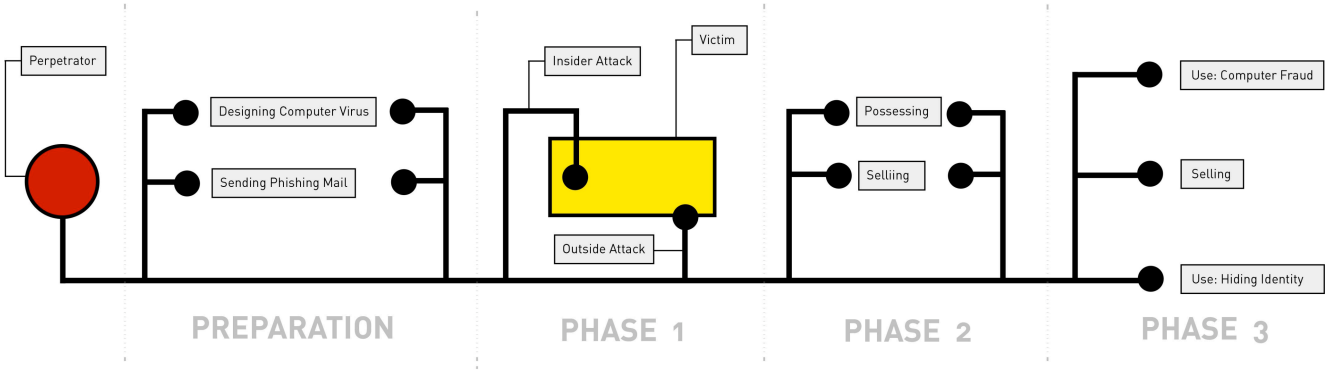
[94] See 2007 identity Fraud Survey Report – Consumer Version, Javelin Strategy & Research, 2007, page 10 – available at: http://www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf (last visited: Nov. 2007).

[95] The two components were pointed out by the Committee on Economic Affairs and Development Report titled "Europe's fight against economic and transnational organised crime: progress or retreat?" (Explanatory Memorandum), 2001: "Using a variety of methods, criminals steal bits and pieces of information about an individual – usually a social security or credit card number or other personal data – and use this information to impersonate their victims and grab as much money as they can." – the Report is available at: http://assembly.coe.int/Documents/WorkingDocs/doc01/EDOC9018.htm (last visited: Nov. 2007).

[96] For an approach to divide between four phases see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 et. seqq. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

- The second phase is characterised by interaction with identity-related information prior to the use of that information within criminal offences (Phase 2). An example is the sale of identity-related information which was obtained by a third person.
- The third phase is the use of the identity-related information in relation to a criminal offence (Phase 3). Examples for such offences can be the falsification of identification documents or credit card fraud.

The Three-Phase Model



4 Current legal approaches

Considering the above analysis, the full criminalisation of identity theft requires the coverage of all three phases.[97] In general there are two possibilities to achieve this aim:

- The creation of one provision that criminalises the act of obtaining, possessing and using identity-related information (for criminal purposes).
- The individual criminalisation of typical acts related to obtaining the identity-related information (such as illegal access, the production and dissemination of malicious software, computer-related forgery, data espionage and data interference), as well as acts related to the possession and use of such information (such as computer-related fraud).

The following chapter gives an overview of examples for both approaches.

4.1 Single provision approach

The most well known examples for single provision approaches are 18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1). The provisions cover all three phases.

4.1.1 The provision

§ 1028 Fraud and related activity in connection with identification documents, authentication features, and information

a) Whoever, in a circumstance described in subsection (c) of this section -
[...]
(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or
[...]

§ 1028A. Aggravated identity theft
(a) Offences.—
(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.
[...]

4.1.2 Phase 1

In order to commit crimes related to identity theft, the offender needs to get in possession of identity-related data.[98] By criminalising the "transfer" of means of identification with the intent to commit an offence, the provisions criminalise the acts

[97] The following overview concentrates on direct criminal sanctions related to Identity Theft. Data protection laws as well as criminal sanctions related to the violation of data protection laws are not covers. Regarding the impact of data protection laws on Identity Theft prevention see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 et. seqq. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf (last visited: Nov. 2007).

[98] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data see above *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007 – available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 (last visited: Nov. 2007); ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf (last visited: Nov. 2007).

related to phase 1 in a very broad way. The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: the transfer of the information from the victim to the offender. Due to the fact that the provisions focus on the transfer act, they do not cover acts undertaken by the offender prior to the initiation of the transfer process.[99] The criminalisation therefore focuses on the final part of phase 1.

The focus of the provisions on the transfer process has another relevant consequence. Due to a lack of a transfer process initiated by the offender, the provision is not applicable if the victim initiates the transfer process. This is especially relevant for phishing scams.

4.1.3 Phase 2

One of the very few common elements of acts related to phase 2 is the fact that the offender is in possession of identity-related information. By criminalising the possession with the intent to commit an offence, the provisions are again undertaking a broad approach with regard to the criminalisation of acts related to phase 2. This includes in particular the possession of identity-related information with the intention to use this later in one of the classic offences related to identity theft.[100]

With regard to the fact that the provisions require the intent to use the data for criminal purposes, the possession of identity-related data without the intent to use them is not covered. Furthermore, it is uncertain whether the provisions criminalise the possession if the offender does not intent to use them but instead sell them.[101]

4.1.4 Phase 3

By criminalising the "use" with the intent to commit an offence, the provisions cover the acts related to phase 3. 18 U.S.C. § 1028(a)(7) is, as mentioned above, not linked to a specific offence (like fraud).

4.1.5 Preparation Phase

As highlighted previously, preparatory acts such as sending out phishing mails and designing malicious software that can be used to obtain computer identity-related data from the victims are not covered by 18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1).

4.1.6 Conclusion

18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1) cover a wide range of offences related to identity theft. The criminalisation is not limited to a certain phase but covers all three phases. Nevertheless, it is important to highlight that the provision does not cover all identity theft related activities – especially not those where the victim and not the offender is acting.

---

[99] Examples for acts that are not covered is the illegal access to a computer system in order to obtain identity related information or

[100] One of the most common ways the obtained information are used are linked to fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

[101] The prosecution could in this case in general be based on fact that 18 U.S.C. § 1028 does not only criminalise the possession with the intent to use it to commit a crime but also to aid or abet any unlawful activity.

4.2 Multiple provision approaches

The following overview does not analyse the status of the related criminal law provisions of each EU member state, but instead focuses on international standards defined by the Council of Europe Convention on Cybercrime,[102] as well as the EU-related Framework Decision on attacks against information systems.[103]

The main difference between the Convention on Cybercrime and other approaches (like for example the US approach) is the fact that the Convention does not define a separate cyber-offence of the unlawful use of identity-related information.[104] Similarly to the situation with regard to the criminalisation of obtaining identity-related information, the Convention does not cover all possible acts related to the unlawful use of personal information. With regard to those acts that are covered by the Convention, the criminalisation is not limited to acts that involve the unlawful use of personal information.

4.2.1 Criminalisation with regard to phase 1

4.2.1.1 Illegal access (Article 2 Convention on Cybercrime) [105]

The Convention on Cybercrime includes a provision on illegal access that protects the integrity of the computer systems by criminalising the unauthorised access to a computer system.

> Article 2 – Illegal access
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The term "access" does not depend on a specific method of communication but is open-ended and subject to further technical developments. It shall include all operations of entering another computer system and covers attacks carried out via the Internet as well as the popular illegal access to wireless networks (WLAN).

With this broad approach the provision covers not just the above mentioned scams but also approaches of perpetrators to enter a computer system in order to obtain identity-related information.

4.2.1.2 Illegal Interception (Article 3 Convention on Cybercrime)

The Convention on Cybercrime includes a provision that protects the integrity of non-public transmission. It criminalises their unauthorised interception, with the aim to

---

[102] Regarding the model law character of the Convention see *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, CRi 2006, 142. Regarding the status of the ratification of the Convention see www.coe.int; Regarding the question in how far the cybercrime-related criminal law legislation in selected EU Member States is already corresponding with the Convention on Cybercrime see the country reports provided by the Council of Europe at www.coe.int.

[103] Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173.

[104] See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29 – available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf (last visited: Nov. 2007);

[105] Art. 2 EU Framework Decision on attacks against Computer Systems is corresponding with Art. 2.

equate the protection of electronic transfers with the protection of voice phone conversations against illegal tapping and recording that currently already exists in most legal systems.[106]

> Article 3 – Illegal interception
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The applicability of Article 3 is limited to the interception of transmissions realised by technical measures. An interception related to electronic data can be defined as any act of acquiring data during a transfer process.[107] The question if illegal access to information stored on a hard disk is covered by the provision is debated.[108] This question particularly concerns the criminalisation of identity theft of great importance. As pointed out further below,[109] it is questionable if the provision covers this act. But the provision is applicable if the perpetrators intercept a data transmission in order to obtain identity-related information.

4.2.1.3 Data interference (Article 4 Convention on Cybercrime)[110]

In Article 4, the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorised interference.

> Article 4 – Data interference
> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
> (2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

The term "damaging" means any act related to the negative alteration of the integrity of information, content of data and programmes. "Deleting" covers acts where the information is removed from the storage media and is considered comparable to the destruction of a corporeal subject.[111] "Suppression" of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.[112] The term "alteration" covers the modification of existing data without necessarily lowering the serviceability of the data. [113]

The "Report on Combating Identity Theft" points out the possibility of data

---

[106] Explanatory Report to the Convention on Cybercrime No. 60.

[107] Within this context only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of "social engineering".

[108] See *Gercke*, The Convention on Cybercrime, MMR 2004, Page 730.

[109] See: 7.1.5.

[110] Art. 4 EU Framework Decision on attacks against Information Systems is corresponding with Art. 4.

[111] Explanatory Report to the Convention on Cybercrime No. 61.

[112] Explanatory Report to the Convention on Cybercrime No. 61.

[113] Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well. .

interference in identity theft cases which involve the use of malicious software.[114] In this case the provision can be used to prosecute perpetrators.

4.2.1.4 System interference (Article 5 Convention on Cybercrime) [115]

In order to protect the interest of operators and users to have appropriate access to telecommunication technology, the Convention on Cybercrime includes in Article 5 a provision that criminalises the intentional hindering of the lawful use of computer systems.

> Article 5 – System interference
> Each Party shall adopt such legislative and other measures as may be necessary to establish an criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

"Hindering" means any act that interferes with the proper functioning of the computer system.[116] The application of the provision is limited to cases where the hindering can be characterised as "serious".[117]

If the act of obtaining the identity-related information is accompanied by the serious hindering of a computer system, the provision can be used to prosecute the perpetrators.

4.2.1.5 Provisional result

The Convention on Cybercrime contains a number of provisions that criminalise Internet-related identity theft acts in phase 1. Taking into consideration the various possibilities of how an offender can get access to the data, it is necessary to point out that not all possible acts in phase 1 are covered. One example of an offence that is often related to phase 1 of the identity theft, but not covered by the Convention on Cybercrime, is data espionage. As mentioned above, the question whether illegal accesses to information stored on a hard disk is covered by Article 3 Convention on Cybercrime is debated.[118]

The discussion is the result of two slightly imprecise explanations in the Explanatory Report to the Convention on Cybercrime. The Explanatory Report first of all points out that the provision covers communication processes taking place within a computer system.[119] But this leaves open whether the provision should only apply in cases where the victim initiated a process that was then intercepted by the perpetrator, or whether it should even apply when the perpetrator himself operates the computer. In addition the Explanatory Report points out that the interception can

---

[114] Combating Identity Theft – A Strategic Plan, US President's Identity Theft Task Force, page 66, 2007 – available at: http://www.idtheft.gov/ (last visited: Nov. 2007).

[115] Art. 3 EU Framework Decision on attacks against Information Systems is corresponding with Art. 5.

[116] Explanatory Report to the Convention on Cybercrime, No. 66.

[117] Although the connotation of "serious" does limit the applicability, it is likely that even serious delays of operations resulting from attacks against a computer system can be covered by the provision.

[118] See *Gercke*, The Convention on Cybercrime, MMR 2004, Page 730.

[119] "The communication in the form of the transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime No. 55.

be committed either indirectly through the use of tapping devices or "through access and use of the computer system".[120]

If a perpetrator gets access to a computer system and uses it to make an unauthorised copy of stored data on an external hard drive, this act leads to a data transfer (sending data from the internal to the external hard disk). Yet this process is not intercepted, but rather initiated by the perpetrator. The missing technical interception is a strong argument against the application of the provision in cases of illegal access to stored information.[121]

4.2.2 Criminalisation with regard to phase 2

4.2.2.1 Misuse of devices (Article 6 Convention on Cybercrime)

There are threats related to the availability of passwords for other data that enable offenders to access a computer system. Facing these threats, the drafters of the Convention decided to establish an independent criminal offence criminalising the illegal interaction with computer passwords, access codes and similar data.

> Article 6 – Misuse of Devices
> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
> (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
>
> > (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
> >
> > (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
>
> (b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
>
> […]

The provision enables the member states not only to criminalise the production or sale but also the possession of such data. It is uncertain whether the provision is applicable with regard to identity theft offences. First of all the provision does not concern identity-related data, but passwords, access codes and similar data. This limits the application of the provision to cases where the identity-related information

---

[120] Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.

[121] Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue see Explanatory Report No. 57: *"The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision."* See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 57.

is a password or an access code.[122] In addition, Article 6 (1)(a)(ii) Convention on Cybercrime requires the intent to use the data for one of the following offences:

- Illegal access to a computer system (Article 2)
- Illegal interception (Article 3)
- Illegal data interference (Article 4)
- Illegal system interference (Article 5)

4.2.2.2 Provisional result

Acts which take place between obtaining the information and using it for criminal purposes can hardly be covered by the Convention on Cybercrime. It is especially not possible to prevent a growing black market for identity-related information by criminalising the sale of such information based on the provisions provided by the Convention.

4.2.3 Criminalisation with regard to phase 3

The Council of Europe Convention on Cybercrime defines a number of cybercrime-related offences. Some of these offences can be committed by the perpetrator by using identity-related information. One example is computer-related fraud, which is often mentioned in context with identity theft.[123]

4.2.3.1 Computer related fraud (Article 8 Convention on Cybercrime)

The Convention seeks to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property by providing an article regarding computer-related fraud.[124]

> Article 8 – Computer-related fraud
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
> a. any input, alteration, deletion or suppression of computer data;
> b. any interference with the functioning of a computer system,
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 8 combines the most relevant acts with regard to computer-related fraud (input, alteration, deletion and suppression) with the general act "interference with the functioning of a computer system" in order to open the provision for further developments.[125]

4.2.3.2 Provisional result

---

[122] An example for an identity-related information that is at the same time an access code is the password to an online banking system. This password enables the offender to access the online banking system of the bank.

[123] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

[124] Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

[125] As a result not only data-related offences but also hardware manipulations are covered by the provision.

Surveys on identity theft point out that most of the obtained data were used for credit card fraud.[126] If the credit card fraud is committed online it is likely that the perpetrator can be prosecuted based on Article 8 of the Convention on Cybercrime. Other offences that can be carried out by using identity-related information that were obtained previously but are not mentioned in the Convention are not covered by the legal framework. It is in particular not possible to prosecute the use of identity-related information with the intention to hide the identity.

4.2.4 Criminalisation with regard to the preparation phase

4.2.4.1 Misuse of devices (Article 6 Convention on Cybercrime)

There are threats related to the availability of devices that can be used to commit cybercrime. Tools that are designed to commit complex offences are available on a large scale on the Internet.[127] Most of the national criminal law systems do, in addition to the "attempt of an offence", contain provisions criminalising acts of preparation of crimes. In general this criminalisation – which involves an extensive forward displacement of criminal liability – is limited to the most serious crimes. Especially in EU legislation there are tendencies to extend the criminalisation for preparatory acts to less grave offences. [128]

Facing these threats, the drafters of the Convention decided to establish an independent criminal offence criminalising specific illegal acts regarding certain devices or access to data to be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data.

> Article 6 – Misuse of Devices
>
> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
>
> (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
>
> (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
>
> (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
>
> (b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

---

[126] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf (last visited: Nov. 2007).

[127] Websense Security Trends Report 2004, page 11 – available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3 – available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[128] An example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

The connecting factors of the criminalisation as established by Paragraph 1 (a) are on the one hand devices[129] designed to commit cybercrimes and on the other hand passwords that enable access to a computer system. With regard to these items, the Convention criminalised a wide range of actions. In addition to production, it sanctions the sale, procurement for use, import, distribution or otherwise making available of the devices and passwords. A similar approach (but limited to devices designed to circumvent technical measures) can be found in EU legislation regarding the harmonisation of copyrights.[130]

If the perpetrators in identity theft cases are producing or possess such devices in order to use them to obtain identity-related information by committing one of the offences mentioned in Articles 2-5 Convention on Cybercrime, they can be prosecuted on this basis.

4.2.4.2 Computer-related forgery (Article 7 Convention on Cybercrime)

Most criminal law systems criminalise the forgery of tangible documents. In protecting the security and reliability of electronic data, the Convention aims to create a parallel offence to the forgery of tangible documents in order to fill gaps in criminal law related to traditional forgery provisions that might not apply to electronically stored data.[131]

---

[129] With it's definition of „distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report No. 72) the drafters of the Convention indicate a restriction of devices to software. Although the Explanatory Report is not certain in this matter it is likely that not only software devices are covered by the provision but hardware tools as well.

[130] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

[131] Explanatory Report to the Council of Europe Convention on Cybercrime No 81: *"The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."*

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

The target of a computer-related forgery is only data – not depending on whether they are directly readable and intelligible. To draw the line on the forgery of tangible documents, Article 7 requires – at least with regard to the mental element – that the data is the equivalent of a public or private document. This includes the need for legal relevance.[132]

The "input" of data corresponds to the production of a false tangible document.[133] In addition to this act, Article 7 lists a number of subsequent actions that correspond to the falsification of a genuine document. With this wide criminalisation, Article 7 covers in particular the falsification of electronic documents (such as emails) in email based phishing scams.

4.2.4.3 Provisional result

The Convention on Cybercrime covers a number of acts related to the preparation of identity theft offences. With regard to the significant number of phishing attacks, the possibility to prosecute the creation as well as sending of phishing mails is of great importance.

4.2.5 Conclusion

The Convention on Cybercrime as well as the EU Framework Decision on Attacks against Information Systems criminalise a number of acts that can be linked to phase 1 and phase 3. With Article 7 of the Convention on Cybercrime, law enforcement agencies are especially able to prosecute email based phishing cases. Nevertheless it is important to point out that neither the Convention on Cybercrime nor the EU Framework Decision contain a general provision covering any approach to illegally obtain, possess or use identity-related information by Internet-related scams.

[132] Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

[133] Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

5 Comparing the approach of the Convention on Cybercrime with the US approach

The Convention on Cybercrime and the criminalisation of identity theft in 18 U.S.C. § 1028 and 18 U.S.C § 1028A are based on two different systems.[134]

§ 1028 and § 1028A create separate offences that – in addition to the offences they are referring to[135] – criminalise the transfer, possession and use of means of an identification of another person with regard to criminal offences.

The Convention on Cybercrime follows a different concept. It does not create a separated offence that criminalises the unlawful use of identity-related information in cybercrime-related cases, but instead criminalises certain acts that are related to identity theft scams.

The major differences between the Convention and the US approach are:

	Convention on Cybercrime	18 U.S.C. § 1028(a)(7)
Criminalisation of Phase 1 -3	The Convention on Cybercrime only criminalises certain acts related to phase 1 – 3 (e.g. the illegal access to a computer system within the process of obtaining the information)	§ 1028(a)(7) follows a broader approach and criminalises extensively identity theft related acts in all three phases
Relevant gaps with regard to internet-related ID-Theft	Especially in phase 2 and 3	No relevant gaps
Criminalisation of preparatory acts	Certain acts covered	Not covered
Applicable to ID-Theft offences that do not include cybercrime	No	Yes

[134] Regarding background information on Identity Theft and Assumption Act of 1998 see: Identity Theft and Assumption Act of 1998 see: : *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 26. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007).

[135] ("any a unlawful activity that constitutes a violation of Federal law" / „any felony violation enumerated in subsection (c)")

6 Conclusions

Identity theft is a threat for Internet users.[136] The fight against perpetrators attempting to obtain and use identity-related information involves a number of challenges for law enforcement and criminal justice.[137]

Analysing the various definitions used to describe the term identity theft as well as the methods of obtaining identity-related data, the type of data the perpetrators are aiming for and the motivations of the perpetrators, shows that the acts that are related to identity theft have very little in common, apart from the fact that the act in general contains three different phases:

(1) obtaining identity-related information;

(2) interacting (possessing, transferring) with them; and finally

(3) using them to commit a crime.

Comparing the US approach to the Convention on Cybercrime as the only international treaty in the area of cybercrime shows significant differences. The main difference is the fact that the provisions of the Convention protect various legal interests, such as the integrity of a computer system, but do not protect the integrity of identity-related information.

As mentioned above, identify theft is in general used for the preparation of further criminal acts, such as computer fraud.[138] Even if identity theft is not criminalised as a separate act, in most countries law enforcement agencies will be able to prosecute the subsequent offences (e.g. computer fraud). The main reason for which some countries have nevertheless decided to criminalise identity theft as a separate offence[139] is the fact that it is often easier to prove the crime of identity theft than the subsequent crimes. Perpetrators can use the obtained identities to hide their own identity. Being able to prosecute the chronologically first act (the identity theft) could avoid difficulties in the identification of the offender carrying out the subsequent acts.

The proposal of the Commission "that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States"[140] is linked to the question on which of the two concepts a legal framework should be based. One possibility would be to supplement the Convention on Cybercrime to close existing gaps. Another approach would be to base the legislative framework on a specific provision that focuses on identity-related information as the subject of legal protection. The advantage of the second approach would be that this covers any form of identity theft, not only if committed through the Internet.

Whatever the results of discussions regarding the criminalisation of identity theft at the European level, it is important to underline that the success in the fight against Internet-related identity theft is not primarily a question of additional substantive law provisions. Other aspects, such as the improvement of international co-operation among law

---

[136] Regarding the economic impact see for example the 2007 Javelin Strategy and Research Identity Fraud Suvey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[137] See above 3.

[138] See *Hoar*, Identity Theft, The Crime of the New Millennium, 2001 – available at: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm.

[139] For an overview about identity theft legislation in Europe see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 et. seqq. – available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; (last visited: Nov. 2007). Legislative Approaches To Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007.

[140] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267.

enforcement agencies – for which the Convention on Cybercrime provides a framework[141] – are of similar relevance. Finally it should be underlined that addressing the problem of identity theft by criminal law provisions is only one of many approaches; other strategies, in particular preventive measures, the education of Internet users, the development of safer identification procedures or the improvement of data protection laws, are equally if not more important.[142]

---

[141] See Art. 23 et seqq Convention on Cybercrime. Regarding the need for international cooperation in the fight against cybercrime see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seqq. – available at: http://media.hoover.org/documents/0817999825_35.pdf; (last visited: Nov. 2007). Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seqq. – available at: http://media.hoover.org/documents/0817999825_1.pdf (last visited: Nov. 2007).

[142] Regarding the data protection approach in the fight against identity theft see: *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415.