FIDIS

Future of Identity in the Information Society

Title:	"D5.3: A Multidisciplinary Article on Identity-related Crime"
Author:	WP5
Editor:	Bert-Jaap Koops (TILT, Netherlands)
Reviewers:	Sabine Delaitre (IPTS, Spain) David-Olivier Jaquet-Chiffelle (VIP, Switzerland)
Identifier:	D5.3
Type:	[Report]
Version:	1.0
Date:	23 May 2007
Status:	[Final]
Class:	[Public]
File:	fidis-wp5-del5.3-identity_related_crime_def.doc

Summary

This deliverable proposes a typology of identity-related crime. From a conceptual, technical, and legal perspective, the numerous manifestations of identity-related crime have been analysed and categorised. The analysis shows that the relationship between attacks on identification systems, types of identity-related crime, and legal provisions is complex. This is important for policy-makers to realise when designing counter-measures to address the threat of identity-related crime.

The report has been written in the form of a multi-disciplinary academic article that has been submitted to a peer-reviewed journal.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	20.07.06	• first integrated version, sections 3-7.1, inserting Martin's draft, extensively edited and expanded (BJK)
0.2	10.08.06	• various minor changes (BJK)
0.3	28.08.06	• introduction, inserted section 2, edited 3-6, created attack tree, footnotes-endnotes (RL)
0.3b	08.09.06	• inserted outlines/ indication of 7.2-7.4
0.4	27.10.06	• various changes (BJK, RL)
0.5	03.11.06	• integrated Nicole's text on countermeasures (RL)
0.6	11.01.07	• completely revised version and final draft for first internal review (BJK)
0.7	27.02.07	• graphics adapted and text adapted (MM, RL); processed comments 1st review (Sabine Delaitre) (BJK, RL) • final version for second internal review (BJK)
0.8	11.05.07	• processed comments from 2nd review (D.O. Jaquet-Chiffelle)
1.0	23.05.07	• final version (BJK)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive Summary	Bert-Jaap Koops (TILT)
2. Text of the article	Bert-Jaap Koops, Ronald Leenes, Nicole van der Meulen (TILT) Martin Meints (ICPP) David-Olivier Jaquet-Chiffelle (VIP)[1]

[1] Jaquet-Chiffelle has been added as an author of the academic article to acknowledge the substantial text suggestions he provided in his internal review of the deliverable. This explains his appearance as both a reviewer and an author.

Table of Contents

1 Executive Summary

This report has been written in the form of a multi-disciplinary academic article that has been submitted to a peer-reviewed journal. FIDIS authors from different disciplines (law, public administration, political science, computer science, and information security) have teamed up to look at identity-related crime from various perspectives.

Identification is ever more important in the online world, and identity-related crime is a growing problem related to this. This new category of crime is not restricted to high-profile instances of identity 'theft' or identity fraud; it is wide-ranging and complex, ranging from identity deletion to unlawful identity creation and identity 'theft'. Commonly accepted definitions are lacking, thus blurring available statistics, and policies to combat this new crime are piecemeal at best. In order to assess the real nature and magnitude of identity-related crime, and to be able to discuss how it can be combated, identity-related crime should be understood in all its aspects. As a first key step, this deliverable introduces a typology of identity-related crime, consisting of conceptual, technical, and legal categories.

The conceptual categories are unlawful forms of identity deletion, identity restoration, and identity change; the latter category is subdivided in unlawful forms of identity takeover ('identity theft'), identity delegation, identity exchange, and identity creation. Identity deletion is subdivided in identification obstruction and identifier erasure.

The technical categories consist of 17 points of attack on identification, ranging from attacks on users of information systems and garbage cans through attacks on computer networks in the various stages in the telecommunication process to attacks on service providers and their systems.

The legal categories distinguishes between identity-specific legal provisions, such as the US crime of identity theft, and identity-neutral legal provisions mainly used in Europe, subdivided in criminal, civil, and administrative provisions.

The analysis shows that the relationship between attacks on identification systems, types of identity-related crime, and legal provisions is complex. This is important for policy-makers to realise when designing counter-measures to address the threat of identity-related crime. The typology can be used as a comprehensive framework for future research, countermeasures, and policies related to identity-related crime.

2 Appendix. Text of the article

A Typology of Identity-related Crime: Conceptual, Technical, and Legal Issues

Bert-Jaap Koops, Ronald Leenes, Martin Meints, Nicole van der Meulen & David-Olivier Jaquet-Chiffelle

Abstract

Identification is ever more important in the online world, and identity-related crime is a growing problem related to this. This new category of crime is not restricted to high-profile instances of identity 'theft' or identity fraud; it is wide-ranging and complex, ranging from identity deletion to unlawful identity creation and identity 'theft'. Commonly accepted definitions are lacking, thus blurring available statistics, and policies to combat this new crime are piecemeal at best. In order to assess the real nature and magnitude of identity-related crime, and to be able to discuss how it can be combated, identity-related crime should be understood in all its aspects. As a first key step, this article introduces a typology of identity-related crime, consisting of conceptual, technical, and legal categories. The conceptual categories are unlawful forms of identity deletion, identity restoration, and identity change; the latter category is subdivided in unlawful forms of identity takeover ('identity theft'), identity delegation, identity exchange, and identity creation. The technical categories consist of 17 points of attack on identification. The legal categories distinguishes between identity-specific legal provisions, such as the US crime of identity theft, and identity-neutral legal provisions mainly used in Europe, subdivided in criminal, civil, and administrative provisions. This typology can be used as a comprehensive framework for future research, countermeasures, and policies related to identity-related crime.

2.1 Introduction[2]

Identity theft, or rather identity 'theft' since identity is not usually taken away from the owner but rather copied, is generally perceived as a growing problem. Although it existed well before the Internet, its growth has accelerated enormously in the Internet era. Especially in the US, a large number of incidents involving identity data, such as social-security numbers and credit-card numbers, have been reported in recent years. The annual losses due to ID 'theft' in the US since 2003 are estimated at $50 billion.[3] Also in Europe, identity 'theft' or, as it is also referred to in Europe, identity-fraud appears in the news on a regular basis and seems to be growing. The UK government repeatedly produced numbers proclaiming annual losses of at least £1.3 billion per year due to ID 'theft' (cf., critically, LSE 2005, pp. 103-109). Media coverage especially relates to phishing scams,[4] 'theft' of identity data such as credit-card numbers from enterprises, etc.

---

[2] This article is the result of co-operative work in the European FP6 Network of Excellence FIDIS (The Future of Identity in the Information Society, http://www.fidis.net). The authors thank Sabine Delaitre (IPTS, Sevilla) for her comments on an earlier version of this article.

[3] According to the White House, in the press release that accompanied the installation of the President's Identity Theft Task Force. See http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html.

[4] Phishing amounts to trying to obtain financial and other personal data of users that can be used, for instance, to access online banking services, by trying to lure them to websites that impersonate those of the user's real bank through cleverly concocted emails. See, e.g., http://www.msnbc.msn.com/id/5184077.

The seemingly growing number of identity 'theft' or fraud should not come as a surprise in the information society. Face-to-face transactions are replaced by ICT-mediated ones, where one's identity is represented by bits and bytes that are relatively easily obtainable by others. Identifiers – the keys to our digital identities, often numbers or usernames – together with a secret (PINs, passwords etc.) unlock access to financial services (e.g., credit-card transactions) or allow services to be obtained (e.g., social-welfare benefits) and so forth. Given the fact that some of these identifiers can be used for multiple purposes, e.g. systems applying single-sign-on, the attractiveness of appropriating them is obvious. What completes the intuitive explanation of the growth of identity 'theft' or fraud is the opacity of what happens with personal data online and the relative inexperience of both users and online service providers in preventing and handling (new) kinds of attacks on personal data.

The importance of identity in the online world is clear and so is the fact that digital identities give rise to identity-related crime. Far less clear is the wide range of crimes that can be committed in relation to identity – identity 'theft' or fraud is actually only one instance of the multi-faceted category of identity-related crime (Koops & Leenes 2006). Moreover, it is also not at all clear what exactly constitutes 'identity 'theft'' or 'identity fraud' and how these can be combated (LSE 2005, p. 98; Leenes 2005, pp. 113-117). This lack of precision becomes especially apparent when comparing the various official and media reports on these topics. Hardly ever are definitions provided, even though the statistics play a role in politically motivated discussions and policy decisions.[5] Also, commonly accepted definitions are lacking in the literature. This means that we are at the stage where comparisons of apples and oranges abound and where it is virtually impossible to determine the real incidence of identity-related crimes.

Thus, in order to assess the nature and magnitude of identity-related crimes, and to be able to discuss how they can be combated, we first need to understand the various phenomena captured under the umbrella term 'identity-related crime'. First key steps to this understanding are clear definitions and a typology of identity-related crime. Building on earlier work concerning definitions (Koops & Leenes 2006), the main aim of this article is to provide a typology of identity-related crime. With 'typology', we mean a classification based on types or categories.[6] We will distinguish three kinds of relevant categories: conceptual, technical, and legal. These categorisations together make up a typology of identity-related crime, which is needed to provide a comprehensive framework for research, countermeasures, and policies related to identity-related crime. To our knowledge, the development of a comprehensive typology has rarely been undertaken in current literature; the best attempt to date (Sproule & Archer 2006)[7] provides useful classifications, but is in our opinion too narrow because it pays less or no attention to types like identity deletion and consensual forms of identity fraud, which fall within our definition of identity-related crime (see section 4).

---

[5] Identity 'theft', for instance plays a significant role in discussions on the introduction of national ID cards (e.g., in the UK, see LSE 2005). More generally, the very nature of the issues at hand – crime, vulnerability, threats, and hence fear – fuels an entire industry that benefits from inflating the terms and accompanying figures to play on public fears; cf., http://www.timesonline.co.uk/article/0,,17129-2022675,00.html.

[6] Cf. *Merriam-Webster Online Dictionary*, http://www.m-w.com/dictionary/typology: 'study of or analysis or classification based on types or categories'.

[7] See also http://www.business.mcmaster.ca/IDTDefinition/defining.htm, where their conceptual model is further developed.

The article is organised as follows. In the following section, we briefly look at identity and communication processes to provide a background for our discussion of identity-related crime. In section 3, we sketch a categorisation of rearrangement of the linkage between persons and identifiers – formulated more easily: 'things you can do to thwart identification' – as the conceptual framework of which identity-related crime is a part. In sections 4 through 6, we describe the conceptual, technical, and legal categorisations of identity-related crime, followed in section 7 by a discussion of the complex relationship between these categorisations. By way of conclusion, we sketch some current initiatives taken to combat identity-related crime, and illustrate how our typology may help in exposing gaps in current approaches.

2.2 Background

2.2.1 Identity

Before we proceed to analyse identity-related crimes, we need to briefly look at identity itself. Identity is a complex concept with, at least, philosophical, cultural, and psychological connotations. A basic distinction relevant here is the one between *idem identity*, i.e., sameness of things or persons, and *ipse identity*, i.e., personal identity in the meaning of an individual's sense of self. In this article, we focus on *idem* identity, the match between an identifier and a natural person (see Hildebrandt, 2007). *Idem* identity needs to be further refined, though. The UK Cabinet Office (Cabinet Office, 2002) distinguishes three elements of identity that can be used to identify an individual:

- *attributed identity*: attributes that are given to a person, usually at birth, such as name, date and place of birth;
- *biometric identity*: attributes that are more or less unique to a person, such as iris, fingerprint, retina, DNA profile, gait, dynamic signature, keystroke behaviour;
- *biographical identity*: attributes that build up over time, consisting of life events and how a person interacts with structured society, including registration of birth, details of education and qualifications, employment history, registration of marriage, mortgage account, and property ownership.

This distinction is not always sharp; identifiers such as credit-card numbers, for instance, are not obtained at birth, but fall somewhere between attributed and biographical identity. In this article, we will use attributed identity to denote the set of all attributes that are given to a person by the state, therefore including identifiers such as national ID numbers and social-security numbers, or by enterprises, such as credit-card numbers or bank account numbers provided by banks.

In addition to the Cabinet Office's aspects, at least one other element of identity should be taken into account:

- *chosen* identity: attributes that are chosen by a person (author pseudonym, nickname, username, password, avatar, etc.).

The four elements of *idem* identity can be classified in various ways, which may help in illuminating strengths and weaknesses of identification processes. For example:

Classification	*More artificial*	*More human-related*
More external	Attributed identity	Biographic Identity
More internal	Chosen identity	Biometric/behavioural Identity

Classification	*Higher stability*	*Higher volatility*
More external	Attributed identity	Biographic Identity
More internal	Biometric/behavioural identity	Chosen Identity

For the purposes of this article, it is useful to see how the elements of *idem* identity relate to crime. Attributed identity data are a prime area for identity-related crime because they generally provide access to services and are also relatively easy to obtain, e.g., by fabricating or stealing documents. Biographical identity relates to 'softer' attributes built up over time, such as employment history. These data are less likely to provide access to valuable services, although they can also be used to lure people into false beliefs that may subsequently facilitate fraud. For instance, a person could fabricate a *curriculum vitae* showing she is a very successful stockbroker, in order to persuade people to let her handle their investment. The third kind of identity data are biometric attributes. The Cabinet's Office report states that these can not be assumed by someone else, but this is incorrect. Some biometrics can be mimicked by others, gait for instance, even though this may be difficult in practice. Other biometrics, such as fingerprints, can be forged and used for fraudulent purposes without knowledge or co-operation of the person the biometric features physically belong to.[8] The fourth kind, chosen identity, contains data that are equally sensitive to identity-related crime as attributed identity, notably user names and passwords; other types of data, such as nicknames or avatars, are not directly prone to facilitate identity-related crime, although theoretically, they might facilitate more exotic forms of crime, such as posting a weblog comment under a renowned pseudonym that belongs to someone else.

2.2.2 Communication steps

Identity-related crime always takes place in a social context: if a (digital) identity is not used in social interactions, then obviously misuse is not an issue. Hence, we start our discussion from the perspective of social systems. In a communicational context, at least three aspects can be important:[9]

- the identity of the participants in the communication (*who*);
- the social system (*where*):[10]
    - organisational, where participants take roles such as members or clients of organisations (e.g., enterprises or governmental agencies);

[8] For a do-it-yourself guide, consult http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en. See also Van der Putte & Keuning 2000 and Geradts & Sommer 2006, p. 28-69.

[9] Sometimes, also the when, why, and what of communications are relevant, but for our purposes of identity-related crime, particularly these three aspects should be taken into account.

[10] For social-system theory, see, e.g., Baecker 1999, Luhmann 2000.

  - interactional, where participants take informal roles that show a certain variety, such as friends, neighbours, etc.;

- the role participants are taking in this specific communicational context (*how*), for example, the role of employee, customer, or teacher.

Usually, to set up a communication, people go through the following steps.

1. *Addressing*: participants in a communication address each other, for example, with a salutation ('Hello Mike!' or 'Mr. President') or other identifiers such as bit strings in the digital world (e.g., e-mail addresses). In some cases, the chosen form also allows to determine which role in which social system the participants are going to take in the communication.
2. *Authentication*: participants check whether the identifier, the social system, and the claimed role properly link to a specific physical person. In the physical world, this is done for example by inspection (looking into each other's eyes or at uniforms, badges, clothing), listening to the tone of voices, interpreting gestures, etc. In the digital world, formalised authentication procedures are used for this.
3. *Authorisation*: participants decide which claims for commitment are connected to the specific communicational context. A close friend, for example, can expect a high level of commitment, while a vendor will not expect this from an unknown customer. The role of a communication partner is important for defining her rights and duties: the same question may have quite different implications when asked by a police officer in function or when asked by her off the record during a game of golf among friends. In the digital world, authorisation is typically implemented based on technically defined roles, for example, in Identity Management Systems (IMS).

Step 1, addressing, is preparatory to identity management, which typically involves authentication and/or authorisation. Errors made in the addressing stage of step 1, also in the punishable sphere, need not be considered as identity-related crimes. For example, when a customer is addressed as 'You filthy Jew, what do you want?' or when a police officer is addressed as 'Hey, motherf***ing scumbag', this does not fit our notions of rearrangement of identity linkage or identity-related crime (see below) and *idem* identity, but rather falls into the category of hate speech and *ipse* identity. Nevertheless, some errors in step 1 may be considered as an identity-related crime, for instance when an e-mail address in a message in transport is changed by a hacker, thereby preventing the message from being delivered (see below on identity blocking).

Steps 2 and 3 lie at the heart of IMS as they are being developed today. They are often taken consecutively in communication processes. Step 2, authentication, establishes familiarity with the identity of the communication partner, and step 3, authorisation, creates familiarity with the role of the communication partner. Step 2 in practice is often skipped when for the purposes of the communication, only the role and not the identity is relevant ('Doctor, I have a headache'). In these cases, problems may arise because of the assumption that the role is actually taken by a person authorised to play the role. For instance, the assumed doctor can be a quack or a con-artist who nevertheless does charge for a consultation concerning the headache.

2.3 A categorisation of rearrangement of identity linkage

There are lawful and unlawful reasons to use a false identity. Publishing under a pseudonym, for instance, is a widely accepted practice; impersonating your neighbour to empty her bank account without her consent is not. In this section, we propose a categorisation that covers both intentional and unintentional, and lawful as well as unlawful types of (mis)using identity. This deepens the understanding of identity-related crime and shows that there are grey areas between criminal and non-criminal activities.

Most definitions and descriptions of identity 'theft' and identity fraud (see below) have one thing in common. Within a specific communicational context, the link between at least one physical person and (a) the name or identifier used and/or (b) the social system and the role taken therein is established in a wrong way. The authentication or authorisation step is passed successfully, but the physical person and the identifier or role in the social system do not match. Authentication in these cases leads to false positives, resulting in a *rearrangement of identity linkage*.

An inverse scenario is also possible, namely of false negatives, creating a different kind of rearrangement of identity linkage. This is when someone has the right identity but fails to be identified, thus preventing the authentication or authorisation step to be passed and preventing the link between person and identifier to be made. This may be done by the identity bearer herself, for instance, when an employee circumvents an identification or authorisation system to enter a building by hopping in behind a colleague while the door is still open. It can also be done by third parties, for example, when someone stealthily applies an RFID blocker to prevent an employee from entering the building with her RFID card. A third commonly observed reason is technical failure, e.g., in the context of biometric systems, leading among other things to False Rejection Rates (FRR). This type can be called *identification obstruction*: intentionally or accidentally blocking the link between person and identifier. It is a subcategory of *identity deletion*, which means deleting the identity of a natural person, through tampering with the identifier of a person or with the linkage between identifier and person. Identification obstruction is usually temporary, but identity deletion can also be more enduring. For instance, instead of an RFID blocker, an attacker can also prevent an employee from entering the building by deleting her record from the database with entry authorisations. We will refer to the on-going deletion by destroying the identifier as *identity erasure*. Identity erasure as such is usually permanent, but the deleted identifier can be re-installed (like the broken link between identifier and person in identification obstruction can be mended). This constitutes another type of rearrangement of identity linkage, namely *identity restoration*. In the case of the employee, this occurs when a system administrator reinserts the employee's name in the database.

We can understand rearrangement of identity linkage independently from any kind of criminal intent. Taking a closer look, one easily discovers that in many cases, rearrangement of identity linkage in fact happens unintentionally or accidentally. An example is confusing in a telephone conversation a daughter with her mother due to the similarity of their voices. This is yet another type to be distinguished: *identity collision* (for further examples and sub-types of identity collision, see Leenes 2006, pp. 51-52). Identity collision is usually discovered by one participant of the communication and resolved. In cases where the collision is not discovered, and stems from a deliberate attempt to confuse the communication partner, identity collision may shift into another category of rearrangement of identity linkage, namely *identity change*.

Identity change is the type most closely related to the notions of identity fraud and identity 'theft', where a false identifier is linked to a person intentionally.

Altogether, we can thus distinguish four types of rearrangement of identity linkage.

- *Identity collision*: a wrong link is accidentally made between an identifier and a person.
- *Identity change*: a wrong link is intentionally made between an identifier and a person (the identifier may be an identifier to an existing person or a newly created one.)
- *Identity deletion*: an identifier linked to a specific physical person is, intentionally or accidentally, deleted by herself or someone else (identifier erasure), or the link between person and identifier fails to be made, through an intentional or accidental act (identification obstruction).
- *Identity restoration*: an identifier previously linked to a specific person and later deleted is, usually intentionally, restored by herself or someone else, or the linkability between an identifier and a person is re-established.

The following figure summarises the main types of rearrangement of identity linkage, which we will refine in more detail in the next section.

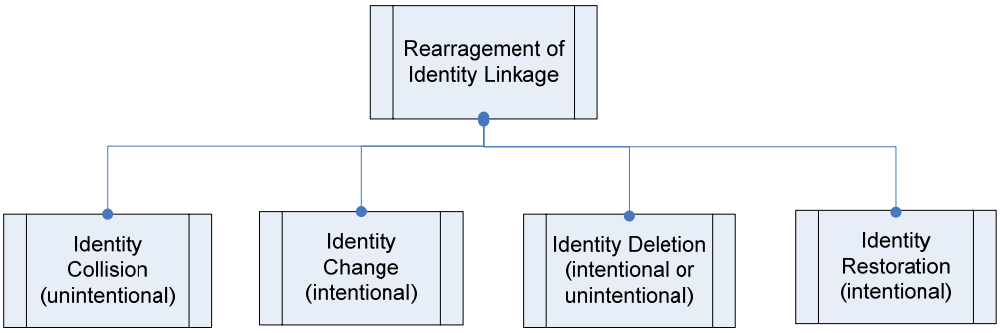

Figure 1: Types of rearrangement of identity linkage

Taking a closer look at identity change, we can distinguish four subcategories, depending on the behaviour of the actor – the non-original identity bearer – and, if present, of the original identity bearer.

- *Identity takeover* or *identity usurpation*: the actor takes over an already existing identity of another person (i.e., the original identity bearer) without this person's consent. In most cases, this identity has already been used in established social structures, so that the step of authentication is passed already or can be passed easily because of known authentication information.
- *Identity delegation* or *identity licensing*: the actor uses an already existing identity of another person with that person's consent; this is similar to identity takeover, but differs in the element of consent.
- *Identity exchange*: two or more people, with mutual consent, use each other's identity; this often happens in already established 1:n relationships, for instance, where two bearers of the same role, e.g., customers, actively exchange identities, such as loyalty cards, in communications with the other communication partner, such as the supermarket.
- *Identity creation*: the actor creates an identity that is, at least to her knowledge, not linked to a physical person. Thus, the actor has to go through authentication and authorisation

procedures by herself. If the created identity accidentally links to an existing person, we have a case of identity collision; in such a case, from the perspective of an independent observer, identity creation may be indistinguishable from identity takeover.

Various motives may lie behind these activities. The actions in all these subcategories of identity change can be perfectly lawful. For example, identity takeover can take place in a hidden-camera program, performed by actors assuming the role of an official or a famous person, or in a parody. Lawful identity delegation occurs when employees authorise colleagues to answer their mail when on holiday, or when a wife lends her bank card to her husband. In most cases of lawful identity delegation, the consent is limited to a certain period and bound to a specific purpose. Lawful identity exchange occurs when Netizens use the CookieCooker (http://www.cookiecooker.de), a cookie-managing program that distributes cookies related to a website randomly between different CookieCooker users with the target to obscure personalised profiles. Finally, identity creation is common in for example multiplayer role games and chatboxes, where 'virtual identities' and pseudonyms abound. However, the actions in these subcategories can also be unlawful, which is the topic of the next section.

2.4 A conceptual categorisation of identity-related crime

'Identity-related crime' can be defined as all punishable activities that have identity as a target or a principal tool (Koops & Leenes 2006). It merits being treated as a distinct, novel category of crime, because combating these crimes requires special knowledge and understanding of identity-management systems and their vulnerabilities, because public awareness should be raised, and because victims suffer from these crimes in special ways, for instance, by being blacklisted.

A categorisation of identity-related crime can be distilled from the categorisation of rearrangement of identity linkage, namely, by distinguishing in all categories a subcategory of unlawful activities.

Identity collision has been defined as happening accidentally; the intentional colliding of identities falls within the category of identity change. Since crime usually involves intent, identity collision will be considered unlawful only in very rare cases. Unintentional acts are occasionally deemed unlawful, notably when a high risk is involved – e.g., accidentally cutting off the power of a hospital – or when someone is in a position, known in German legal doctrine as *Garantenstellung*, where she ought to be particularly careful; for example, a system administrator in a power plant is punishable if she accidentally uploads a program with a virus. Applying this to identity collision, someone might be considered to act unlawfully if she has the same name as a contentious public figure, such as Ayaan Hirsi Ali, and writes during the climax of cartoon-gate in a blog that she will visit Cairo next week, forgetting to mention that she is not the famous politician, and thus accidentally causes violent demonstrations in Cairo resulting in deaths of several by-standers. As she ought to have known that this was a possible result, she could be held liable through criminal law or tort. This admittedly is a far-fetched example, suggesting that the category of unlawful identity collision is small indeed and had presumably better be left out of the typology of identity-related crime.

Identity deletion is a more relevant category from a criminal perspective. When someone has (part of) her identity deleted by someone else or when identification is blocked, this can have severe consequences, for instance, when a hacker destroys patient records in a hospital

computer system. For such an act to fall within the scope of 'identity-related crime', however, the destruction of the patient record should be done with the goal of destroying a patient's identity. Otherwise, it simply is a matter of data interference[11] that need not be labelled '*identity*-related crime'. Most instances of unlawful identity deletion will actually fall in traditional categories of crime (e.g., damage to property, data interference, slander). Nevertheless, it is useful for legislatures to analyse whether intentionally erasing someone else's (partial) identity or intentionally blocking identification merits specific criminalisation, given that people can hardly function within (a sector of) society if their existence in (sectoral) files and computer systems is denied.

When someone destroys (part of) her own identity, this may well be considered unlawful; several countries, for instance, have criminalised destroying an official ID, and they consider it unacceptable when asylum seekers destroy their passport before arrival. However, as Rost, Meints, and Hansen rightly point out (Leenes 2006, p. 55), the latter could be seen as building up a new identity rather than merely destroying an old identity, and this could therefore be dealt with in the category of identity change.

Identity restoration is usually perfectly acceptable, and will normally be done by the identity bearer herself. The prototypical example is Mark Twain, who, after having been proclaimed dead by a newspaper, told the world that reports of his death were grossly exaggerated. Unlawful identity restoration may, however, occur when someone reinstalls part of her identity without right, for example, when a physician with a disciplinary prohibition to work in the medical field reassumes the role of physician, thus misleading the public, or when an ex-Beatle announces a solo performance under the name of The Beatles. These examples suggest that unlawful identity restoration by the identity bearer usually involves roles rather than identifiers. When identity is restored by someone else without the consent or knowledge of the person whose identity is being restored, this may be unlawful as well. If an ex-mafia criminal, having served as a crown witness, has received a new identity in a witness protection program (which is lawful identity creation), it would be unlawful identity restoration to make public the link between the 'new' physical person and his old, ex-mafia, identity, thus putting his life at risk.

Altogether, the above categories can be thought of as overseeable and minor phenomena when compared to the category of *identity change*. It is enticing to equate unlawful identity change with 'identity fraud', because many uses of identity change indeed boil down to fraud. This risks neglecting the fact that unlawful identity change can also be driven by non-economic motives, and hence not all misuse amounts to fraud in the usual penal sense.[12] One may, for instance want to use someone's identity to harm his reputation, or to let someone else in for a crime, for example by giving, when drunk, another's name to a police officer stopping your car; this, in the US, is usually called 'criminal identity theft' (PRC 2002). Nevertheless, the major part of unlawful identity change typically contains an element of fraud. We therefore call the category of unlawful identity change 'identity fraud', defined as fraud or another unlawful activity committed with identity as a target or principal tool (based

---

[11] See art. 4 of the Council of Europe's Convention on Cybercrime, [online] Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm: the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right.

[12] Cf., the definition of computer-related fraud in art. 8 Convention on Cybercrime: 'causing (...) a loss of property to another person (...) with fraudulent or dishonest intent of procuring, without right, an *economic benefit* for oneself or for another person' (italics added).

on Koops & Leenes 2006). Each of the four subcategories of identity change has a substantial unlawful subcategory.

Unlawful identity delegation occurs, for example, when a director gives the password to her digital signature to her secretary to sign documents he is not authorised to sign, or when David Beckham authorises a look-alike to open a new supermarket and to share the considerable fee offered by the supermarket between them. *Unlawful identity exchange* can take the form of someone visiting his brother in prison and remaining behind while the convict walks out, or – depending on the terms and conditions – of customers swapping loyalty cards to thwart a supermarket's profiling. *Unlawful identity creation* occurs when, for instance, someone uses a self-generated credit-card number that fulfils the characteristics of credit-card numbers.

Most importantly, *unlawful identity takeover* is when someone uses the identity of an existing person without that person's consent, for some unlawful purpose. This is what is usually called 'identity theft': fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent. 'Identity theft' is a rather awkward term, since identity is not something that is typically stolen. A characteristic of theft, after all, is that the owner no longer possesses the stolen thing. With identity, this is usually not the case: the victim of identity takeover still retains her identity, or so we hope. We should therefore speak of 'identity "theft"' rather than of 'identity theft' (Koops & Leenes 2006).

On the basis of the distinctions we have made, the following – conceptual – categorisation is established of all forms of rearrangement of identity linkage and identity-related crime.

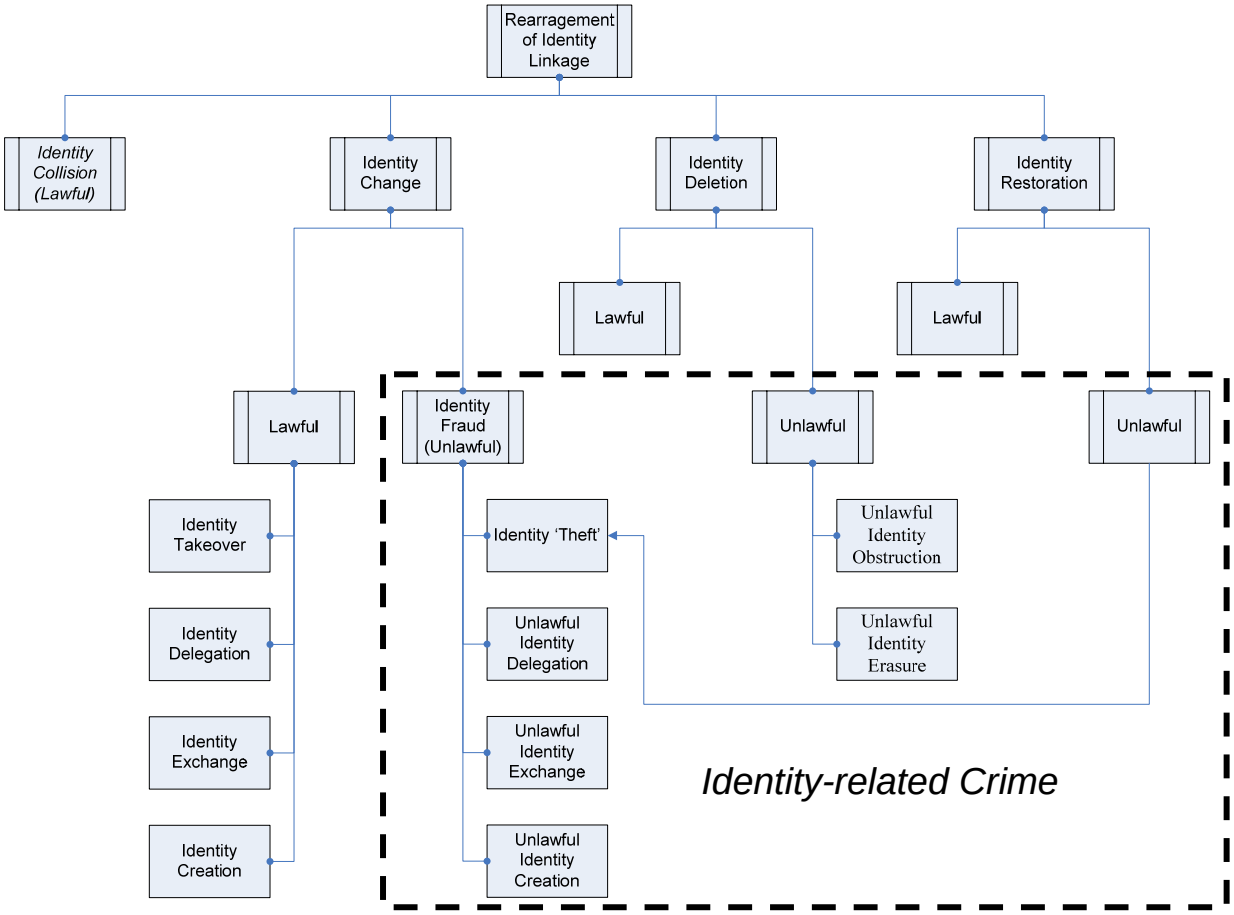

Figure 2: Categorisation of rearrangement of identity linkage and identity-related crime

This categorisation clarifies what constitutes identity-related crime, as a subcategory of rearrangement of identity linkage, at a conceptual level. This is a necessary first step in understanding identity-related crime, but it is only a beginning. In real life, after all, crimes are not committed through concepts, but through – often technical – tools and activities. If we are to combat identity-related crime, we therefore need to understand not only what type of crime is being committed, but also *how* it is committed. This calls for a categorisation of attacks on identification, which is technical in character.

2.5 A technical categorisation of identity-related crime: identification attacks

In identity-related crime, an established authentication and/or authorisation procedure is passed successfully while it should not have been (false positives), or is not passed successfully while it should have been (false negatives), in both cases because the link between the identifier and the right physical person is broken due to rearrangement of identity linkage. Criminals can exploit various points of attack to cause such a rearrangement and perform this in various ways, e.g., directed at a specific person, or undirected in relation to many, unselected persons. For an analysis of various techniques, we refer to Leenes (2006, pp. 84-86).

A first basic distinction is that identity-related crime, at least the most prevalent ones in the category of identity fraud, is essentially a two-stage process. The first stage involves – lawfully or unlawfully – gathering identity data of others or creating new identity data. The second stage is using these data in some unlawful way. Sometimes, more subdivisions are made in the literature, but these two stages are common to all analyses of identity fraud (Leenes 2006, p. 114).

Helpful as this distinction in two stages is, it gives little understanding of all the ways in which identity-related crime can be committed in practice. Since this distinction only addresses the identity-fraud part of identity-related crime, but not identity deletion or identity restoration, we have opted for another kind of categorisation of identity-crime techniques. In order to better understand the diversity of attacks and their relation with our conceptual categorisation (section 4), we explore these in more detail by considering the following simplified picture of online interactions. This allows us to determine the various points of attack and hence to uncover vulnerabilities in identification mechanisms.

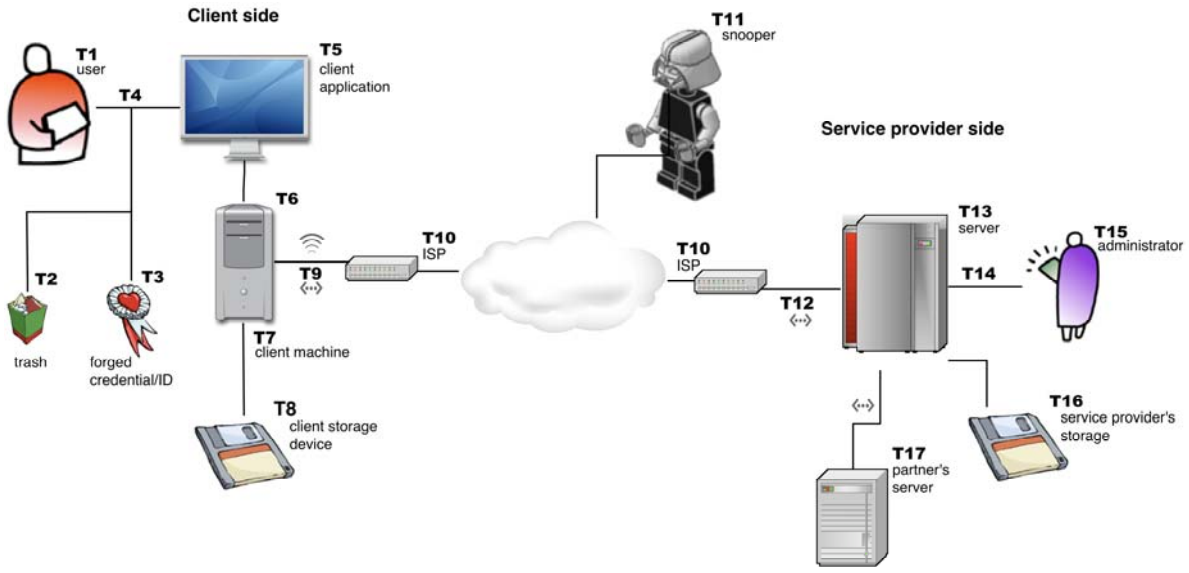

Figure 3. General view of online interactions showing 17 points of attack

The threats are the following.

T1 is a direct attack on the user, for instance by threatening her to make her disclose identity data, by applying social engineering, such as phishing attacks, by stealing credit cards from a wallet, or even by replacing the individual by a look-alike.[13]

T2 is 'dumpster diving': an attack on identity data people leave behind in the physical world, such as user names and passwords written on post-it notes, receipts of account details in the garbage can, or forensically scanning second-hand PCs for remaining identity data.

T3 represents the creation of forged identity data or credentials, for instance by acquiring a credit card with self-generated identity data, or forging a medical diploma.

T4 is any attack on the communication between users and their IT systems, such as their PC. This includes *malware phishing* (Levy 2004), like keystroke loggers, presenting faked biometric data e.g., a Synthetic Biometric Feature Attack, and intercepting or interfering with Bluetooth communication between keyboard and PC.

T5 is the manipulation of user applications such as web browsers, to record data entered by the user, e.g., through Trojan horses, or to redirect the user to fake websites, by spoofing attack. The reading of cookies set in the user's browser is another example of this kind of attack.

T6 relates to the interception and manipulation of data at the level of the operating system, for instance, by viruses, root-kits, and spyware.

T7 concerns attacks on the client's PC itself, like intrusion by hackers or the installation of physical devices, such as modified hardware.

T8 are attacks on the link between the user's PC and storage devices, both internal ones and external ones like USB sticks, with the goal of obtaining or redirecting identity data.

[13] According to a recent report, 7% of the convicts in Dutch prisons are not who they claim to be (Grijpink 2006, p. 45).

T9 are attacks on the communication channel between the user's system and the internet, for instance interception of WiFi signals from a user's home, or using the user's WiFi installation to obtain a communication channel.

T10 are attacks on Internet Service Providers involved in the communication, for instance, by spoofing DNS entries resulting in the redirection of the user's communication to a rogue site.

T11 represent attacks on the network, for example, man-in-the-middle attacks, wiretapping, node redirection, denial-of-service attacks, or cyberterrorism.

T12 is analogous to T9, as also the service provider's internal network can be attacked by snoopers and sniffers – network infiltration.

T13 are attacks on the service provider's IT system, such as hacking into the service provider's databases.

T14 is symmetrical to T4, concerning any attack on the communication between the system administrator and the service provider's IT system, for instance, by installing key-loggers or root-kits.

T15 represents physical or logical attacks on or by the service provider's staff; personnel leaking identity data to outsiders is an example.

T16 involves any attack on the service provider's data storage, like the La Salle Bank backup tapes that went missing in December 2005.[14]

T17 concerns attacks on the communication between service providers and their business partners, like a bank or accountant.

In principle, all possible cases of identity-related crimes involve one or more of the threats outlined. The categorisation shows the wide variety of possible attacks and *modi operandi* in identity-related crime. This is important to bear in mind when devising countermeasures, since a chain is as strong as its weakest link. This means that a risk assessment is necessary that covers all potential points of attack. It would be useful, in that respect, to have data available on the actual risks involved in the various attacks, i.e., the likelihood – or actual incidence in the past – of an attack and the associated expected – or real suffered – loss. This is a topic for further research.

2.6 A legal categorisation of identity-related crime

The categorisations of concepts and attacks provide a good basis for analysing and combating identity-related crime. Still, we feel a need to add one more categorisation, namely of legal provisions. This is required to analyse one of the most obvious countermeasures, namely criminalisation. The problem is that, like criminals, criminal law tends not to abide by neat, conceptual distinctions, and unlike criminals, it often disregards *modi operandi* and defines crimes regardless of the way they are committed. And besides criminal law, also civil law (tort) and administrative law (data-protection infringements, for example, or giving a false identity in a naturalisation request) are legal countermeasures to be considered. Both the concepts and the attacks do not match neatly one-to-one unlawful activities as defined in law

[14] See http://securitypronews.com/insiderreports/insider/spn-49-200512222005TheYearInIDFraud.html.

(for brevity's sake, we will refer to unlawful activities hereafter as crimes). If we want to know the occurrence of identity-related crime in real life, we need to know which criminal and other legal provisions are used for which types, since available statistics are usually based on the crime for which people are convicted, not on the attacks they used or on the conceptual category of the concrete crime.

Not all the attacks will be punishable (criminal law) or otherwise unlawful (tort, administrative law) in practice. This depends, after all, on the existing legal context. Moreover, not all types in our conceptual categorisation need necessarily be criminalised; what is considered undesirable or criminal behaviour still depends to a considerable extent on social, cultural, and legal norms that vary from country to country. For example, the United States and European countries to date have varying approaches with respect to identity-related crime.

In the United States, the Identity Theft and Assumption Deterrence Act specifically covers identity-related crime, albeit largely restricted to identity 'theft'.[15] This penalises anyone who 'knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.'

In European countries, there is – to our knowledge – no specific criminal provision targeting identity 'theft' or identity fraud as such (cf., Koops 2005), nor do the Council of Europe's Convention on Cybercrime[16] or the EU Framework Decision on attacks against information systems[17] contain identity-specific crimes. Some countries do have special provisions targeting specific subcategories of identity-related crime, such as deletion or forgery of official identity documents,[18] but a general criminalisation of identity 'theft', identity fraud, or other types of identity-related crime is absent. Instead, countries largely rely on non-identity-specific, and often traditional, criminal provisions, such as fraud, forgery, data damage, illegal access to data, or imposture.

A major distinction in a legal categorisation of identity-related crime, then, is identity-specific versus identity-neutral crimes. Within identity-neutral crimes, major subdivisions can be made between criminal, civil, and administrative law, and between specific provisions, like fraud, and general provisions, such as aiding and abetting. This leads us to the following overview. [See **Figure 4** in Appendix]

This is a tentative, not-exhaustive categorisation – it is not easy to create a definitive categorisation for legal provisions, since there is no international standard or relevant treaty and since provisions differ from country to country. Nevertheless, the basic distinctions in this categorisation are relevant for all countries, and many of the identity-neutral types will feature in most countries' legislation. As such, the categorisation can be used by countries to detect potential gaps in their legislation with respect to identity-related crime.

---

[15] U.S. Identity Theft and Assumption Deterrence Act, Public Law 105-318, 112 STAT. 3010, 30 October 1998, codified at 18 U.S.C. § 1028(a)(7).

[16] Supra, note 11.

[17] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal* L 69/67, 16.3.2005.

[18] See, for instance, articles 347-350 Estonian Criminal Code, as mentioned in the FIDIS ID Law Survey, [online] Available at http://idls.law.uvt.nl.

2.7 Mapping the three categorisations

The relationship between attacks on identification systems, types of identity-related crime, and legal provisions is complex. This becomes immediately apparent when trying to map the conceptual, technical, and legal categorisations on each other. A many-dimensional structure is required to adequately represent the complex relationships, which is not possible on two-dimensional paper. We will confine ourselves to illustrating the interrelations in a far-from-exhaustive table, mapping the attacks on identification to types of identity-related crime and legal provisions. For the latter category, it should be realised that actual punishability depends on the national context and the actual specifics of the case. Further note that the *modus operandi* mentioned does not necessarily fulfil all the requirements of the crime category; often, it concerns the preparation of identity 'theft' by collecting data, not necessarily leading to identity 'theft' itself, which, in our definition, involves the *use* of such data.

Type of attack	**Example of *modus operandi***	**Type of identity-related crime**	**Legal provisions**	**Comment**
T1	Social engineering	- (preparation of identity 'theft')	preparation of fraud; privacy infringement; imposture; identity theft (US)	Using a plausible case and role context, authentication data is taken from members in organisations
T1	Phishing	- (preparation of identity 'theft')	preparation of fraud; intellectual-property infringement; preparation of identity theft (US)	Use of fake email messages, sms, etc., to make users enter identification data on faked websites
T1	Generation of an alibi for an identical twin	unlawful identity exchange	obstructing a criminal investigation; perjury; criminal identity theft (US)	
T1	Destroying a passport	identity deletion	damage to official documents	
T2	Dumpster diving	- (preparation of identity 'theft')	-	Usually not unlawful as such
T3	Generation of credit-card information for non-existing credit cards	unlawful identity creation	preparation of fraud	Online-payment was possible, though no corresponding bank account existed, before the current additional validation number was introduced and used

Type of attack	Example of *modus operandi*	Type of identity-related crime	Legal provisions	Comment
T3	Generation of faked serial numbers of ID documents	unlawful identity creation	preparation of forgery	This is used for example to prove one's age in the context of Internet transactions
T3	Usurpation of office, false assumption of authority	unlawful identity creation	imposture; fraud; identity theft (US)	
T4	Viruses installing a key logger	- (preparation of identity 'theft')	data interference; hacking; illegal interception of communications	Logged authentication data are used to perform identity theft
T4	Readout of authentication data	- (preparation of identity 'theft')	fraud; imposture; identity theft (US)	
T5	Pharming	- (preparation of identity 'theft')	hacking; data interference; preparation of fraud; intellectual-property infringement; preparation of identity theft (US)	Altering domain-name information to attract victims to fake websites.
T6	installing a root kit	- (preparation of identity 'theft')	hacking; data interference; preparation of fraud; preparation of identity theft (US)	Root kits can be used to report certain kinds of data to their master.
T7	Installing a hardware key-logger	- (preparation of identity 'theft')	trespassing; hacking; illegal interception	
T8	Stealing a USB stick	- (preparation of identity 'theft')	theft	
T9	Using someone's home WiFi network to send hate speech under that person's name	identity 'theft'	hate speech; illegal access; imposture; slander; criminal identity theft (US)	
T10	Spoofing DNS system to redirect to phishing	- (preparation	hacking; data interference	

Type of attack	Example of *modus operandi*	Type of identity-related crime	Legal provisions	Comment
	site	of identity 'theft')		
T11	Spoofing of biometric sensor without co-operation of the original identity bearer	identity 'theft'	fraud; forgery; imposture; identity theft (US)	
T11	Man-in-the-middle attack[19]	identity 'theft' or preparation thereof	imposture; data interference; illegal interception; hacking	
T12	Denial-of-service attack on bank's website	identity obstruction	computer sabotage	
T13	Wrong death notice in a public paper	unlawful identity deletion	slander	
T13	Manipulation of reference data in identity management systems	- (preparation of identity 'theft')	forgery; preparation of fraud; data interference	
T14	Installing key logger at webshop to intercept credit-card numbers	- (preparation of identity 'theft')	hacking; data interference; illegal interception; preparation of fraud	
T15	Passing along of authentication data by members of organisations to outsiders	unlawful identity delegation	aiding and abetting fraud; identity theft (US)	
T16	Use of personal data of dead persons	unlawful identity restoration; identity 'theft'	fraud	

Table 1: Types of attack and corresponding concepts and legal provisions

[19] See for example http://md.hudora.de/jura/rechtstatsachen/node31.html, http://en.wikipedia.org/wiki/Man_in_the_middle_attack, and Schneier 1996.

It is equally relevant to draft similar tables that map the concepts to attacks and legal provisions, and that map legal provisions to the concepts and attacks, but that exceeds the scope of this article.

The relevance of this exercise is that it shows the multi-facetedness of identity-related crime, which is a key insight in the fight against this form of crime. The table shows that many attacks exist in stage 1 (see beginning of section 5), the preparatory stage in which identity data are collected or created, which can subsequently be used in a stage 2 attack on an identification system in order to attain some unlawful goal. In combating identity-related crime, focusing on stage 1 activities is therefore equally important as, if not more important than, focusing on the unlawful use of identities. This brings us to the final question of our article: how can the three categorisations help in devising strategies for combating identity-related crime?

2.8 Conclusion: addressing identity-related crime

It is not the aim of the article to analyse current initiatives to combat identity-related crime; we refer to other studies providing overviews (Gill et al. 2006; Van der Meulen 2006). Here, we restrict ourselves to noticing that the strategies – if existent at all – seem partial at best. Although the United States seems to be more developed than most European countries in initiatives to combat identity-related crime, both in criminalisation and public-awareness campaigns (cf., Van der Meulen 2006), the US approach is largely restricted to identity 'theft' and therefore tends to overlook other types, such as unlawful identity deletion and unlawful identity exchange or delegation. In the EU, some policy measures have been proposed, but these are quite limited and also largely restricted to financial identity 'theft' (European Commission 2004; Van der Meulen 2006, pp. 21-22). A striking reverse example is the Netherlands, where policy documents tend to focus on look-alike fraud with ID documents and giving false identification data in asylum procedures, but where – at least at the government level – financial identity 'theft' receives less attention. Our conceptual categorisation helps in showing the partial nature of these approaches and determining possible gaps in counter-strategies.

This is particularly relevant since counter-strategies should integrate technical, organisational, and legal measures (Leenes 2006, pp. 116-118). It is not for nothing that we call identity-related crime a new type of crime that merits separate attention (*supra*, section 4): many types of identity-related crimes can be committed by similar *modi operandi*, and they may be facilitated by similar vulnerabilities in identity-management systems. An integrated approach is needed to determine the weakest links in identification management and to devise the most effective and efficient countermeasures. Here, the technical categorisation of identification attacks and the legal categorisation of identity-crime-related legal provisions can serve as tools to analyse these weaknesses and countermeasures.

To illustrate this, we briefly survey several countermeasures currently taken by governments or suggested in academic literature. The initial target of these often appears to be the perpetrator. In the United States, for example, the first policy initiative focused on criminalising identity 'theft'. Over the years, however, many have argued for the ineffectiveness of fighting identity 'theft' simply through criminalisation. Pontell, for example, argued how '[t]rying to deal with identity fraud through criminalization alone, cannot serve as an effective means of control' (Pontell 2002, p. 14). Solove provided a more

extensive argument: '[u]nderstanding identity theft in this manner—as a form of criminal activity to be stamped out through criminal law—misconstrues the problem in a profound way. (...) Identity theft is a consequence of an architecture, one that creates a series of vulnerabilities. This architecture is not created by identity thieves; rather, it is exploited by them' (Solove 2004, p. 4). Thus, the target of policy initiatives needs to shift from the perpetrators of the crime to the (in)direct enablers of the crime.

Both policy makers and authors have recognised how increasing corporate liability and responsibility is another valid option in the fight against identity fraud. Bruce Schneier describes how 'network security is a business problem. The only way to fix it is to concentrate on the business motivations. We need to change the economic costs and benefits of security. We need to make the organizations in the best position to fix the problem want to fix the problem' (Schneier 2004, p.4). Because security is often far from a business priority, several US states have introduced breach-notification laws, requiring organisations to notify individuals when their personal information has been compromised. Some argue, however, that such laws are unnecessary and may cause more harm by forcing consumers to be notified even when no potential damage is envisioned; consumers could thus become desensitised and as a result, when there is a serious breach, would not take any precautionary measures.

Another element in the technical-organisational sphere is introducing better methods of verification. Lopucki claims 'that creditors and credit-reporting agencies often lack both the means and the incentives to correctly identify the persons who seek credit from them or whom they report' (Lopucki 2001, p. 94), but this is only partially correct. Creditors and credit-reporting agencies, at least in the US, lack the incentive to correctly identify users, although the means certainly exist. From a cost-benefit perspective, however, it is currently more advantageous for creditors and credit-reporting agencies to continue existing practice, as their costs of identity 'theft' do not outweigh their costs of increased security. At the same time, from the consumers' perspective, there is a trade-off between enhanced security and user-friendliness: using multi-barrier identification measures, i.e., two or more identification mechanisms rather than single ones, enhances security but is likely not to be adopted by users, unless strongly pressured by governments to adopt them (Mitchison et al. 2004, p. 29).

Consumers, then, also need to be targeted by initiatives. Raising public awareness is an essential element of the overall fight against identity 'theft'. As Johnson notes, however, '[i]t is important to recognize that public education efforts can only go so far with combating the growth of identity crime. Because social-security numbers (SSNs), in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim' (Johnson 2004, p. 56).

This brings us to a final remark illustrating the failure of current piecemeal approaches. The Dutch focus on identity fraud as look-alike fraud and asylum-seeker fraud imply that countermeasures are limited to ID documents. At the same time, the Dutch legislator introduced a unique citizen number, the 'Citizen Service Number', to be used broadly within government, rather mirroring the US social-security number, and thus severely enlarging the risk of financial identity fraud and identity 'theft'. Since this type of identity-related crime was not prominent in the legislator's mind, the risk was almost completely disregarded despite warnings by the Council of State and the Data Protection Authority (Van der Meulen, pp. 26-27).

Our brief scan of countermeasures suggests that there is yet much work to do in combating identity-related crime. The conceptual, technical, and legal categorisations outlined in this article can assist researchers and policy makers in this task, by providing a comprehensive framework that covers all relevant aspects to be taken into account.

2.9 References

Baecker, D. (1999), *Organisation als System*, Suhrkamp, Frankfurt am Main.

Cabinet Office, Identity Fraud: a study, July 2002, http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf

European Commission (2004), A New EU Action Plan 2004-2007 to Prevent Fraud on Non-cash Means of Payment, COM (2004) 679 final, Brussels, 20.10.2004.

Geradts, Z. & Sommer, P. (eds.) (2006), *Forensic Implications of Identity Management Systems*, January 2006, FIDIS deliverable D6.1, available via http://www.fidis.net.

Gill, M. et al. (2006), *The Fight Against Identity Fraud: A Brief Study of the EU, the UK, France, Germany, and the Netherlands*, Perpetuity Research & Consultancy International Ltd.

Grijpink, J.H.A.M. (2006), 'Identiteitsfraude en overheid', *Justitiële verkenningen*, vol. 32, no. 7, pp. 37-57.

Hildebrandt, M. (2007), 'Profiling and the Identity of the European citizen', in: M. Hildebrandt & S. Gutwirth (eds.), *Profiling the European Citizen. Cross-disciplinary perspectives*, Springer 2007, Chapter 15 (to appear).

Koops, B.J. (2005), *FIDIS Deliverable D5.1: A survey on legislation on ID theft in the EU and a number of other countries*, [online] Available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.1.law_survey.pdf.

Koops, B.J. & Leenes, R.E. (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions Matter', *Datenschutz und Datensicherheit*, vol. 30, no. 9, pp. 553-556.

Leenes, R. (ed.) (2006), *FIDIS Deliverable D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research*, [online] Available at http://www.fidis.net/487.0.html.

Levy, E. (2004), Criminals become Tech Savvy, *IEEE Security and Privacy*, 02(2):65-68.

LSE (2005), *The Identity Project: an assessment of the UK Identity Cards Bill and its Implications. Version 1.09*, LSE, London, [online] available at http://is2.lse.ac.uk/idcard/identityreport.pdf.

Luhmann, N. (2000), *Organisation und Entscheidung*, 1st Edition, Westdeutscher Verlag, Opladen/Wiesbaden.

Mitchison, N. et al. (2004), *Identity Theft: A Discussion Paper*, European Commission Joint Research Center, March 2004, [online] Available at https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

Privacy Rights Clearinghouse (PRC) (2002), *Factsheet 17(g). Criminal Identity Theft* (revised May 2002), [online] Available at http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm.

Schneier, B. (1996), *Applied Cryptography*, 2nd Edition, John Wiley & Sons, New York.

Schreurs, W, Hildebrandt, M, Gasson, M., Warwick, M. (eds) (2006), Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence, FIDIS D7.3.

Solove, D. J. (2003), Identity Theft, Privacy, and the Architecture of Vulnerability, *Hastings Law Journal*, Vol. 54, p. 1227-1273.

Sproule, S. & Archer, N. (2006), *Defining Identity Theft – A Discussion Paper*, 6 April 2006, available via http://www.business.mcmaster.ca/IDTDefinition/lit&links.htm.

Van der Meulen, N. (2006), *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union*, Tilburg, 6 September 2006, [online] Available at http://www.tilburguniversity.nl/intervict/publications/NicolevanderMeulen.pdf.

Van der Putte, T. & Keuning, J. (2000), Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, in *4th Int. IFIP wg 8.8 Conf. Smart card research and advanced application (CARDIS)*, eds. J. Domingo-Ferrer and D. Chan and A. Watson, Kluwer Academic Publishers, Boston, etc., pp. 289-303.

Appendix. Figure 4

<table>
<tr><th>Identity-specific</th><th colspan="5">Identity-neutral</th></tr>
<tr><td>Identity-related Crime</td><td>Criminal – general</td><td colspan="2">Criminal – specific</td><td colspan="2">Civil</td><td>Administrative</td></tr>
<tr><td>Identity theft</td><td rowspan="2">Criminal preparation</td><td colspan="2">Illegal interception, illegal access to data</td><td colspan="2" rowspan="2">Tort</td><td rowspan="5">Administrative</td></tr>
<tr><td>Identity fraud</td><td colspan="2">Hacking</td></tr>
<tr><td>Identity forgery</td><td rowspan="3">Attempt</td><td>Damage to property</td><td>Computer sabotage
Data manipulation</td><td rowspan="3">Intellectual-property infringement</td></tr>
<tr><td rowspan="2">Imposture</td><td colspan="2">Theft</td></tr>
<tr><td rowspan="3">Aiding and abetting</td><td>Fraud</td><td>Computer-related fraud</td><td colspan="2" rowspan="2">Data-protection infringement</td></tr>
<tr><td></td><td rowspan="2">ID deletion</td><td>Forgery</td><td>Computer-related forgery</td></tr>
<tr><td colspan="2">Other</td><td colspan="2">Other infringement</td></tr>
</table>

Figure 4. Legal Categorisation of Identity-related Crime

The grey areas denote activities that are often more related to stage 1: identity establishment; the white areas are often more related to stage 2: unlawful use of identity.