8 Identity-Related Crime and Forensics

Bert-Jaap Koops and Zeno Geradts*

Summary. With the ever-increasing importance of identity and identity management in the information society, identity-related crime is also on the rise. Combating crimes like identity theft and identity fraud, not in the least with the help of identity forensics, is a key challenge for policy makers. This chapter aims at contributing to addressing that challenge. It summarises the findings of five years of FIDIS research on identity-related crime and identity forensics. A typology is given of the various forms of identity-related crime. After an analysis of relevant socio-economic, cultural, technical, and legal aspects of identity-related crime, potential countermeasures are discussed. We then move on to forensic aspects, with a critical analysis of pitfalls in forensic identification and case studies of mobile networks and biometric devices. Next, forensic profiling is discussed from a wide range of perspectives. The chapter concludes with lessons drawn from the five years of FIDIS research in the area of identity-related crime and forensic aspects of identity.

8.1 Introduction

This chapter summarizes the findings of five years of FIDIS research on identity-related crime and identity forensics.[1] We present the insights gained into the various forms in which identity-related crime can take place, and analyze their socio-economic, technical, and legal aspects. We then move on to identity forensics, with a critical analysis of pitfalls in forensic identification, and forensic profiling.

In the past five years of FIDIS research, we have moved forward significantly in our understanding of the concepts, tools, and legal aspects of identity crimes

* Bert-Jaap Koops is responsible for sections 1, 2, and 5 of this chapter. Zeno Geradts is responsible for sections 3 and 4 of this chapter.

1 We acknowledge here the collective effort of a large group of FIDIS researchers. Key insights were provided by David-Olivier Jaquet-Chiffelle (VIP), Mark Gasson (READING), Ronald Leenes (TILT), Martin Meints (ICPP), Nicole van der Meulen (TILT), Róbert Pintér (ISTRI), Martin Rost (ICPP), and Peter Sommer (LSE). Other contributors included Vicky Andronikou, Sebastian Clauß, Mihály Csótó, Fanny Coudert, Sabine Delaitre, Ekaterina de Vries, Hans Graux, Mireille Hildebrandt, Sylvia Ioset, Attila Kincsei, Mathias Kirchner, Els Kindt, Klaus Kursawe, Mieke Loncke, Ioannis Maghiros, Svetla Nikova, Árpád Rab, Maren Raguse, Falk Wagner, Rikkert Zoun and Albin Zuccato.

and forensics. At the same time, we observe that the field is moving fast, and that key challenges lie ahead to keep up with developments in technology and society. With the ever increasing importance of identity and identity management in the information society, it is clear that combating identity-related crime, not in the least with the help of identity forensics, is a key challenge for policy makers. This chapter aims at contributing to addressing that challenge.

8.2 Identity-Related Crime

8.2.1 The FIDIS Taxonomy of Identity-Related Crime[2]

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. Moreover, it is also not at all clear what exactly constitutes 'identity "theft"' or 'identity fraud'. This lack of precision becomes especially apparent when comparing the various official and media reports on these topics. Not often are definitions provided, even though statistics play a role in politically motivated discussions and policy decisions, for example, to introduce ID cards. Commonly accepted definitions are also lacking in literature. This means that we are at the stage where comparisons of apples and oranges abound making it 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'. Paramount to this understanding are clear definitions and a typology of identity-related crime. FIDIS has developed a comprehensive taxonomy of identity-related crime, as a basis for further research and policy on combating identity crimes.

To our knowledge, such a comprehensive framework is a novelty. Sproule & Archer (2006) provide useful classifications, and De Vries et al. (2007) propose a definition of identity fraud based on an extensive literature review, but these are too narrow because they pay little attention to types like identity deletion and consensual forms of identity fraud, which are part of the identity-related crime landscape.

Categories of Mismatches Between Identifier and Identity

To understand the nature of identity-related crime, it is useful to realize that there are lawful and unlawful cases where some kind of mismatch occurs between identifier and identity. Publishing under a pseudonym, for instance, is a widely accepted practice; impersonating one's neighbour to empty her bank account without her consent is not. A taxonomy should therefore include categories of mismatches between iden-

[2] This section is based on FIDIS Deliverables D5.2b (Leenes, 2006) and D5.3 (Koops et al., 2009), and on Koops and Leenes (2006).

tifier and identity that cover both intentional and unintentional, and lawful as well as unlawful types of (mis)using identity. In our analysis, we take the perspective of an observer of the identification process. This provides a more objective view on the issues than taking other possible perspectives such as that of the individual whose identity is being (mis)used or that of the person or institution suffering a loss.

Most definitions and descriptions of identity 'theft' and identity fraud (see below) have in common that, within a specific communication context, the link between at least one individual and (a) the identifier used and / or (b) the social system and the role taken therein is established incorrectly. Authentication in these cases leads to false positives, the individual is unjustly identified: individual and the identifier or role in the social system do not match. The reverse, false negatives, is also possible: the individual is unjustly not identified. In this case the link between individual and identifier is not made or blocked. This may be caused by the individual herself, who may, for instance, circumvent her employer's identification or authorization system by slipping in behind a colleague while the door is still open. More common is identity obstruction by others. A felon may, for instance, secretly apply an RFID blocker to prevent the employee from entering the building with her RFID card. Technical failures are also common causes for identity obstruction.

Identity obstruction has two subcategories. The first is identification obstruction, which means blocking the identification process in the identifying system, for example with an RFID blocker; this is usually temporary. The second is identifier erasure, which is usually (more) permanent; for instance, instead of using an RFID blocker, the attacker may bar the employee from entering the building by deleting her access control record. Although the second is a more lasting form of obstruction, the deleted identifier can of course sometimes be re-instantiated (e.g., restoring the access control record), thus inversing identity erasure: identity restoration.

The mismatch of identifier and individual can be understood independently of criminal intent. In many cases the mismatch in fact happens unintentionally or accidentally. An example is mistaking a daughter for her mother in a telephone conversation due to the similarity of their voices. This example reveals a third type of identity rearrangement: identity collision. Identity collision is usually discovered by one of the communicating partners and subsequently resolved. When the collision remains undiscovered, and is caused deliberately, identity collision may shift into 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 problems regarding the link between identifier and individual.

- *Identity collision*: a wrong link is *accidentally* made between identifier and individual.
- *Identity change*: a wrong link is *intentionally* made between identifier and individual (the identifier may be an identifier to an existing individual or a newly created one.)

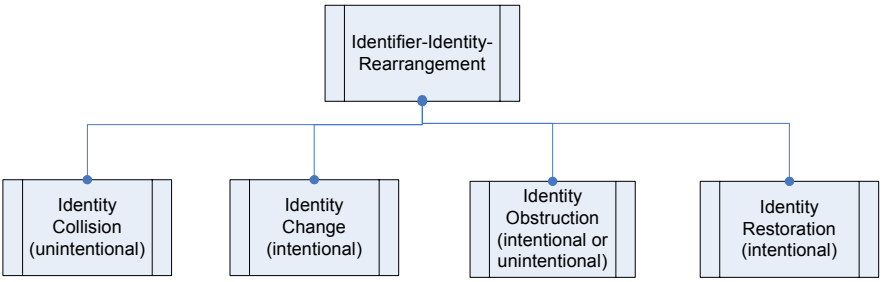

Fig. 8.1. Types of identifier-identity rearrangement

- *Identity obstruction*: an identifier linked to a specific individual is, intentionally or accidentally, deleted by herself or someone else (identifier erasure), or the link between individual and identifier fails to be made, through an intentional or accidental act (identification obstruction).
- *Identity restoration*: a deleted identifier is, usually intentionally, restored by the individual or someone else, or the linkability between identifier and individual is re-established.

Figure 8.1 summarizes the main types of rearrangement of identity linkage, which will be refined in more detail below.

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 existing identity of another individual (i.e., the original identity bearer) without this individual's consent. In most cases, the acquired identity was already established in a certain social structure; authentication therefore already took place or can easily be carried out because the required information already exists.
- *Identity delegation* or *identity licensing*: the actor uses an existing identity of another individual with her consent; this is similar to identity takeover, apart from the element of consent.
- *Identity exchange*: two or more individuals, with mutual consent, use each other's identity; this often happens in established 1:n relationships, for instance, customers (role) swapping loyalty cards in a supermarket.
- *Identity creation*: the actor creates an identity that is, at least to her knowledge, not linked to an existing individual. If the created identity accidentally links to an existing person, this constitutes identity collision, which, from the perspective of an independent observer, may be indistinguishable from identity takeover.

The actions in all these subcategories of identity change may be perfectly legal. For example, identity takeover can take the form of an actor assuming an official's role as part of a hidden-camera program or in a parody. Employees commonly authorize colleagues to answer their mail when on holiday (lawful identity delegation). In most cases of lawful identity delegation, consent is limited to a certain period and bound to a specific purpose.

CookieCooker (http://www.cookiecooker.de) provides a form of lawful identity exchange distributing one's webcookies randomly between different users with the aim of obscuring personalized profiles. Finally, identity creation is common in multiplayer role games and chatboxes where many users use pseudonyms. However, the actions in these subcategories can also be unlawful, which is the topic of the next section.

Categories 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 and 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 victims suffer from these crimes in special ways, for instance, by being blacklisted, and because public awareness is low and should be raised.

The categories of identifier-identity mismatches allow us to construct a categorization of identity-related crimes. Each type of rearrangement has lawful and unlawful instances (Figure 8.2).

Identity collision was defined as accidental (intentional identity collision falls within the category of identity change). Since crime usually requires intent, identity collision is unlawful only in 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 where she ought to be particularly careful (Garantenstellung in German legal doctrine); for example, system administrators in a power plant are punishable if they accidentally upload programs with a virus. We have found no real cases of unlawful identity collision, suggesting that this category is small indeed, even if possible in practice.

Identity obstruction is a more relevant category from a criminal perspective. When someone has (part of) her identifier deleted by someone else or when identification is blocked, this can have severe consequences; think of a hacker destroying patient records in a hospital computer system. For such an act to fall within the scope of 'identity-related crime', however, the destruction of a patient record should be done with the goal of destroying their identity, else it would be data interference.[3] Most instances of unlawful identity obstruction actually constitute traditional crime categories (e.g., damage to property, data interference, slander). Nevertheless, given the fact that people can hardly function within society if their existence in

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

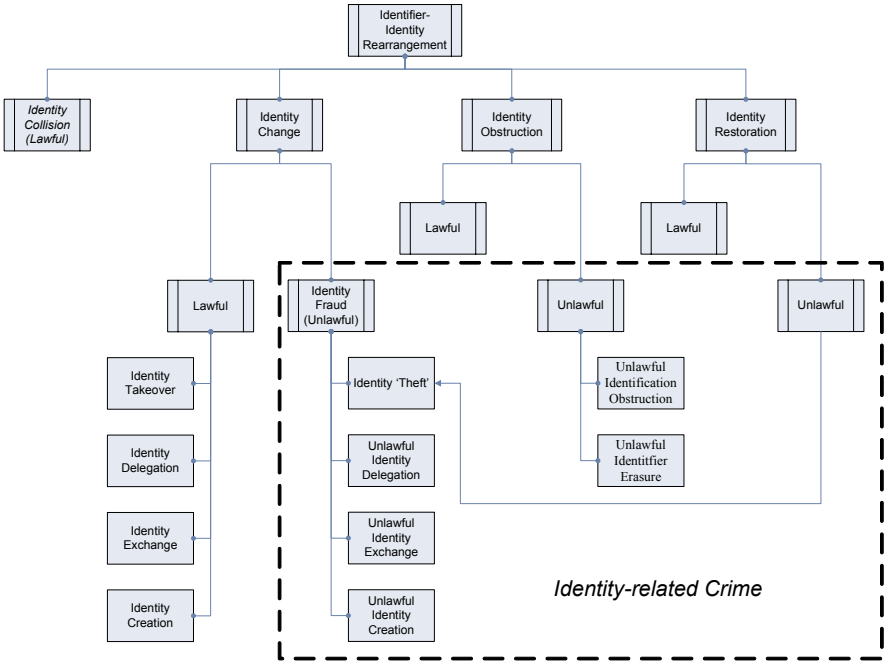

Fig. 8.2. Types of identifier-identity rearrangement and identity-related crime

computer records is denied, it may be useful to consider criminalizing intentionally erasing someone else's (partial) identifier or intentionally blocking identification. Destroying (part of) one's own identifier is considered unlawful in several countries. Germany, for instance, has criminalized destroying an official ID, considering it unacceptable when asylum seekers destroy their passport before arrival. Interestingly, the latter act could also be construed as building up a new identity (identity change) rather than destroying an old one (Leenes, 2006: 55).

Identity restoration is usually perfectly acceptable. 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. An example of unlawful identity restoration, however, is a physician with a disciplinary prohibition to practice who resumes his practice, thus misleading the public. Unlawful identity restoration by the identity bearer usually involves roles rather than identifiers. Also forms of unlawful identity restoration by third parties without consent or knowledge of the individual involved exist. If an ex-mafia criminal who turned crown witness has received a new identity in a witness protection program (which is lawful identity creation), then making the link between him, his former and his new identity public, thereby endangering him, would constitute unlawful identity restoration. Incidentally, if the ex-criminal resorts to his former identity himself, this may also be deemed unlawful, because in many countries, civic identities are unique and defined by the state.

The preceding categories are minor phenomena when compared to the category of identity change. Although unlawful identity change often aims at committing fraud for financial gain,[4] this is not always the case. Fraud can also result in other types of damage.[5] Examples are the use of someone's identity to harm their reputation or providing a false name when stopped by a police officer to let someone else in for a criminal offense, such as drinking and driving. The latter behaviour is usually called 'criminal identity theft' in the United States.[6] Because most cases of unlawful identity change contain an element of fraud, we call this category 'identity fraud', defined as fraud (in the broad sense of unlawful deception resulting in some kind of injury to another person) committed with identity as a target or principal tool.

Each of the four subcategories of identity change has a substantial unlawful subcategory. We provide some examples. Unlawful identity delegation: a medical practitioner who provides her digital credentials to an assistant to process patient data on her behalf, which is unlawful in many countries. Unlawful identity exchange: someone visiting an inmate in prison and remaining behind while the convict walks out.[7] Unlawful identity creation: someone uses a self-generated credit-card number that fulfils the characteristics of credit-card numbers. Unlawful identity takeover in our view is what is usually called 'identity theft': fraud 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; unlike theft, where the owner loses possession over the stolen good, the victim of identity takeover still retains her identity. We should therefore speak of 'identity "theft"' rather than of 'identity theft' (Koops and Leenes, 2006).

Identity-related crime, certainly in the category of identity fraud, is often described (see, e.g., De Vries, 2007; Leenes, 2006: 114) as a two-stage process. The first stage involves – lawfully or unlawfully – gathering identifying data of a specific individual or unspecified individuals in a group of potential victims, or creating new identifying data. The second stage involves using these data in some unlawful way. While useful, this two-stage distinction does not provide much insight in the mechanics of identity-related crimes, how they are committed, nor into ways to combat them. Before we analyze those aspects in more detail, we will have a look at the occurrence of identity-related crime, both as portrayed in the media and in real life.

---

[4] 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).

[5] Cf., Webster's definition: 'intentional deception resulting in injury to another person', http://www.websters-online-dictionary.org/definition/fraud.

[6] See http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm.

[7] This is actually a problem in Dutch prisons, see Grijpink (2006).

8.2.2 Aspects of Identity-Related Crime

Identity-Related Crime in Films[8]

It may look odd to start a further discussion of identity-related crime with a section on films, but it is important to realize that the media is very influential in the way in which an issue is perceived and framed. When identity obstruction is mentioned, people may think first of Sandra Bullock's character in The Net being erased from society, and identity 'theft' raises the image of The Talented Mr. Ripley completely taking over the identity of his victim. The average person most often comes across the issue of identity-related crime, and identity 'theft' in particular, in mass culture indirectly rather than personally. Identity 'theft' and other forms of identity-related crime are indeed a permanent feature in mass culture, since identity and its integrity, preservation, and protection from others forms an integral part of the human mind and society.

It is therefore important to examine how identity-related crime features in mainstream films, particularly since media theory suggests that films constitute reality as source of information and have an educating effect on people (Pintér, 2007: 9-10). Films, as much as real-world stories, influence the perception of identity crimes and thus, indirectly, public policies that are always partly based on general perceptions.

Films draw on primeval stories and fears at least as much as on technological trends and topical situations. Roles and identities, as well as the changes these have undergone have existed ever since the earliest forms of society. In the Middle Ages, the concealment of identity and the "casting off" of traditional roles existed in regulated forms, notably the Carnival where roles were swapped during a few days of madness (allowing firm role establishment during the rest of the year). In modern times, where individuality and the associated importance of identity and liberty have come to the forefront, role and identity play have become more varied and common.

Throughout history, identity change has been an inexhaustible source of humour, but it was also important in fairy tales with a moral message to teach. These days, identity change as a source of humour still exists (e.g., Robin Williams in Mrs. Doubtfire), but the moral teaching element has largely disappeared. Besides humour, however, identity change as a possible source of crime has increasingly come into the limelight, with fear and suspension as prime factors in identity crimes facilitated by technology. This approach has been intensifying in the period of digital reality and digital identities, now it has become easier than ever before to assume another person's role, for example through plastic surgery (Face / Off) or the use of another person's data (Filofax), or the use and misuse of another's account (The Net).

A survey of international mainstream films, categorized according to the FIDIS taxonomy (Section 8.2.1), shows that identity collision (e.g., Working Girl, where the initial accidental collision gradually turns into identity takeover), identity deletion (e.g., The Net), and identity restoration (e.g., The Bourne Identity) occur much less frequently than identity change. Particularly identity 'theft' is a productive

[8] This section is based on FIDIS deliverable D5.2c (Pintér, 2007).

theme (e.g., Fantômas, Auggie Rose), but also delegation (e.g., Dave), exchange (e.g., Trading Places), and creation (e.g., Johnny Handsome) occur frequently.

The picture of identity-related crime suggested by films, however, is mostly misleading. Films, especially mainstream, mass-cultural products, oversimplify the issue and depict it as if victims have no means to defend themselves and are entirely at the mercy and whim of identity 'thieves'. These films focus on the rare cases where the targeted individual falls victim to fraud, is robbed of his identity, and is completely replaced in society by the identity 'thief'. Contrary to reality, this emerges as a standard or prototypical form of identity 'theft' in films. This is understandable, since such a plot is more interesting, exciting, and more effective on the screen as compared with the bulk of bank-account takeover and other abuses taking place in reality. The bulk of real-life identity 'theft' cases cause financial damage but do not completely disrupt the social life of the victims. In reality, invisible criminals do not strive to completely destroy their victims' personalities and identities; rather, they try to "simply" make money out of their crime without being seen or shedding blood. Such cases are unsuitable for mainstream films.

As a result, whoever receives their information mainly from films will form a false picture of identity-related crime and may remove the issue into the realms of fiction and the world of urban legends. The bias of films to focus on extreme and unrealistic cases therefore poses a risk that current trends in identity-related crime and legal, organizational, and technical countermeasures are underdeveloped in citizens' world views.

Given the importance of awareness-raising to combat identity-related crime, it is vital that actions are taken to adjust the picture of identity-related crime, in particular identity 'theft', as it is sketched in the media at large. Film producers could contribute to this by showing standard data-security measures, such as a virus check, as part of everyday life. However, films are not likely in future to sketch a substantially different picture of identity 'theft', given the primeval appeal of extreme identity takeover as a theme in visually mediated fiction. The required readjustment of the picture of identity-related crime will therefore have to rely on other mass-media, such as non-fiction literature and documentaries, the press, and blogs.

Identity-Related Crime in Real Life[9]

In the United States, 'identity theft' has become a household word, and the media continues to tell fear-igniting stories of stolen identities. The actual size of the problem, however, is contested, so that identity 'theft' might be a hype rather than a big problem in real life in the US. In recent years, the problem – or the hype – and the subsequent need for policies and countermeasures have spread from the US to other areas, including Europe. The extent of the problem in Europe is unknown. Rather than relying on (contested) US data and concerns – which may or may not be quite specific for the US situation – a description of actual European prevalence of identity crimes would help put our concerns about identity 'theft' in perspective.

[9] This section is based on FIDIS deliverable D12.7 (Van der Meulen and Koops, 2008).

We have tried to provide such a picture by shedding light on the situation in Belgium, France, Germany, and the United Kingdom, these being EU member states that have a policy debate about identity-related crime, so that a certain amount of reports and data are available. This provides a first indication of the prevalence of identity 'theft' in Europe, on which subsequent studies can build. The resulting picture is, unfortunately, only a piecemeal one: studies appear scarce, and most authors point out that the lack of a separate criminal provision makes it more complicated to gather information on the problem, since crimes are not being specifically reported or registered as identity-related crime. Moreover, uncertainty and unclarity about definitions are dominating themes in many reports with regard to identity 'theft'. The unclarity about definitions and about the actual prevalence of identity 'theft' prevent policy makers, or so they claim, from taking action.

Nevertheless, the contours of a picture of the European prevalence of identity-related crime shimmer through the available data and reports. Document fraud is an on-going concern, with tens of thousands of cases yearly in countries like Belgium and France. The traditional forms of document forgery have been supplemented more recently with look-alike fraud, which is a major concern in several countries.

However, in the past few years, a shift has occurred from document and look-alike fraud to online forms of fraud, in particular financial identity fraud or identity 'theft'. Phishing – which traditionally relies on luring ICT users by deceptive email messages to false websites – seems to be increasingly replaced by covert forms of fraud, in particular by botnets that assemble identity and personal data from infected computers.

Altogether, identity-related crime, particularly document forgery, look-alike fraud, and computer-related financial identity 'theft', is a significant form of crime that is on the rise. There is insufficient empirical evidence to call it a big problem yet, but the upward trend warrants taking expeditious measures to prevent it becoming a big problem in the first place. In order to know which measures are most appropriate, it is useful to have a further look at the ways in which these forms of crime can be committed.

Technical Aspects: Modes of Attack[10]

To deepen our understanding of identity related crimes it helps to study possible points of attacks, vulnerabilities, and types of attack. For this purpose, we make use of the following simplified picture of online interactions (Figure 8.3).

The threats and examples of their use are as follows.

T1 is a direct attack on the user: threatening them to make them disclose identity data; applying social engineering, such as phishing attacks; stealing credit cards from a wallet; replacing the individual by a look-alike.

[10] This section is based on FIDIS deliverables D5.2b (Leenes, 2006) and D5.3 (Koops et al., 2009).

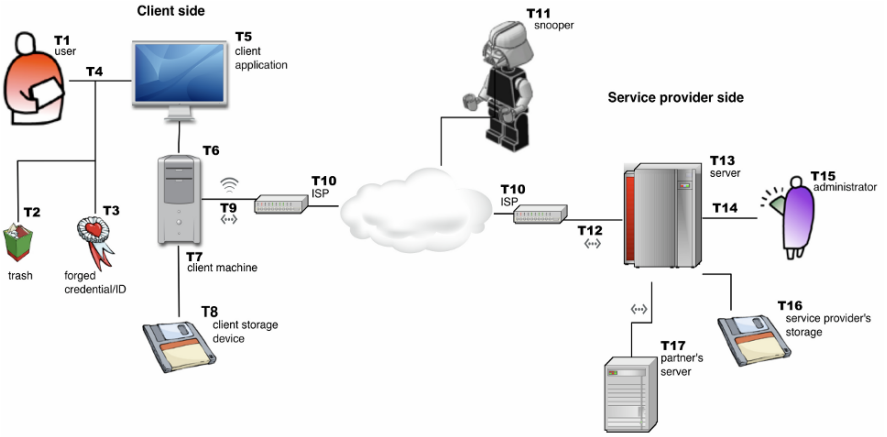

Fig. 8.3. General view of online interactions showing 17 points of attack

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

T3 represents the creation of forged identity data or credentials: generating identity data to acquire a credit card; 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, like keystroke loggers, presenting forged biometric data, 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 through spoofing. Reading cookies set in the user's browser is another example.

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

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

T8 are attacks on the link between the user's PC and storage devices (hard disks and USB sticks), aimed at obtaining or redirecting identity data.

T9 are attacks on the communication channel between the user's system and the internet: interception or manipulation of WiFi signals from a user's home.

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

T11 represent attacks on the network: man-in-the-middle attacks; wiretapping; node redirection; denial-of-service attacks.

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

T13 are attacks on the service provider's IT system: 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.

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

T16 involves any attack on the service provider's data storage.

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

This list shows the wide variety of possible attacks and modi operandi in identity-related crime. In principle, all possible cases of identity-related crimes involve one or more of the threats outlined. In order to assess actual risks in interactions and devise countermeasures, it would be useful to have empirical data on the likelihood or actual incidence. As emerges from the previous section, attacks like T3 (document forgery) and T6 (botnets to phish for data) are prevalent, but altogether, extensive empirical evidence on where attacks actually take place is sparse and anecdotal.

Legal Aspects: Relevant Legal Provisions[11]

The various types of identity-related crime are, by our definition, unlawful. Which attacks and modi operandi actually are unlawful, and what kind of sanction can be imposed, however, depends on a country's legislation. Relevant provisions can be found in multiple legal subdomains, such as criminal law (e.g., hacking), civil law (e.g., tort), and administrative law (e.g., giving a false identity in a naturalization request). Relevant regulation, such as data-protection regulation, often belongs to multiple legal domains (criminal law, administrative law). Furthermore, criminal law tends not to abide by neat, conceptual distinctions, and often disregards modi operandi and defines crimes regardless of the way they are committed. This also shows in the statistics. In the case of criminal convictions, available statistics usually report the crime for which people are convicted, not the attacks they used nor the conceptual category of the concrete crime. And finally, there are few interna-

[11] This section is based on FIDIS deliverables D5.1 (Koops, 2005) and D5.3 (Koops et al., 2009).

tional standards and relevant international treaties to facilitate cross-jurisdictional comparisons.

Not all attacks outlined in the previous section are punishable (criminal law) or otherwise unlawful (tort, administrative law) in practice. Whether they are depends on the existing legal context, i.e., jurisdiction and existing legislation. Moreover, not all types in our conceptual categorization need necessarily be criminalized; 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'.[12] This penalizes 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 – hardly any specific criminal provision targeting identity 'theft' or identity fraud as such, nor do the Council of Europe's Convention on Cybercrime[13] or the EU Framework Decision on attacks against information systems[14] 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,[15] but a general criminalization 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.

The legal categories of identity-related crime can be divided in identity-specific and identity-neutral crimes. Many identity-neutral provisions can actually be used to sanction identity-related crimes, in criminal, civil, and administrative law. Traditional criminal provisions unspecific to identity, like forgery, fraud, and theft, can be used, possibly in combination with general provisions about aiding and abetting or criminal attempt. Also, the traditional identity-specific crime of imposture might be relevant. For a tentative, non-exhaustive categorization that maps possible identity-neutral and identity-specific provisions that can be found in most jurisdictions, we refer to Koops et al. (2009). This overview could be used to detect potential gaps in national jurisdictions with respect to identity-related crime.

---

[12] 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).

[13] Supra, note 3.

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

[15] See, for instance, articles 347-350 Estonian Criminal Code, as mentioned in the FIDIS *ID Law Survey*, available at http://www.fidis.net.

Countermeasures[16]

As we have seen, the United States have in the Identity Theft and Assumption Deterrence Act specifically criminalized identity 'theft'. They have taken several other countermeasures to combat identity-related crime, often through legislation. These include the Gramm-Leach-Bliley Act that imposes security measures on organizations, laws such as the Fair and Accurate Credit Transactions Act (FACTA), which increase organizational responsibility, and security breach notification laws.

Like the US, European countries are also taking countermeasures to combat identity-related crimes. Rather surprisingly in view of regulatory traditions, in Europe, legal measures are much less prominent than in the United States. As noted, criminal law has not been adapted in European countries to accommodate identity crimes specifically. Other legislative measures taken in the US, like free credit reports, seem rather specific to the US situation. Some measures, for example mandatory truncation of credit card numbers on receipts, may nevertheless be valuable in Europe as well. Particularly laws requiring security breach notification have recently also become an issue in Europe. Such a system requires organizations to provide their customers with notification whenever they have lost personal information. This is a promising measure, although the danger of individuals becoming immune to frequent notifications must be taken into account.

Measures like those imposed in the US by legislation are often taken by the financial sector itself, or by public-private partnerships, in Europe. Financial institutions are acutely aware of the threat of identity 'theft', and they take the lead in enhanced technical and organizational security measures. Unlike in the US, these do not necessarily have to be backed up by legislation. A wide panorama of measures is visible, consisting of awareness raising campaigns, complaint centers, and innovative technical measures like virtual dynamic cards or enhanced transaction authentication numbers. Some potential solutions, however, are opposed by merchants and banks for economic reasons, suggesting that market failure – one of the reasons for the US to impose legal obligations – may not altogether be absent in Europe.

Welcome as all these countermeasures are, there is a snag. One countermeasure consistently showing up is to introduce general-purpose electronic identity cards and numbers, often backed up by biometrics, aimed at preventing document or look-alike fraud. The downside of such measures is that they introduce considerable vulnerabilities: as the resulting identification infrastructure comes to rely heavily on the unique eID method, the risk of identity 'theft' actually rises, and the burden of proving being a victim of identity 'theft' becomes heavier as the system is supposedly more secure. Thus, general-purpose eID cards and numbers to curb document fraud are a two-edged sword, and governments need to carefully consider and monitor emerging side-effects.[17]

[16] This section is based on FIDIS deliverable D12.7 (Van der Meulen and Koops, 2008).

[17] See also FIDIS deliverable D13.3 (Buitelaar, 2007) and Section 9.2 of this book.

8.3 Forensic Implications[18]

We have focused so far on identity-related crime, analyzing its concepts and techniques and indicating legal, organizational, and technical measures to combat crimes in which identity is used as a target or principal tool. Much of the knowledge relevant to understand identity-related crime is also relevant to its mirror image: identity forensics. Identifying perpetrators is one of the key functions of forensics, and given the increasing importance of identity management, identity forensics is a major field of study in the information society.

The term forensic, as used in this chapter, refers to information that is used in court or other dispute resolution procedures as evidence. Such information can be extracted from identification management systems. This evidence can be very strong, however some limitations are apparent. For example, one should always investigate if identity change has been committed as shown in Figure 8.2.

8.3.1 Forensic Aspects

For forensic science, it is important to know the reliability of the identity management system, and that the evidence extracted from the system can be explained in court, where the model as discussed in Figure 8.2 can be used. We distinguish the following issues:

Reliability of Underlying Technology

How good is the technology, and is it easy to alter, copy, reproduce etc. the data that identifies a certain person? In forensic science it is important to understand the underlying technology that is used. For example how easy is it to alter an image of a person which is used as evidence in a crime case.

How Well Is the Individual Bound to an ID Artifact?

It is often quite easy to exchange paper passports. In the case of look-alike fraud, another person can use a passport at the border without anyone realizing it. Furthermore, in some countries it is relatively simple to switch identity, by asking the government for a change of names.

Auditability

Can we audit the complete system and determine how it works, for example an ATM system? Do we have log records of for example a payment system?

[18] This section is based on FIDIS deliverables D6.1 (Geradts and Sommer, 2006) and D6.7c (Geradts and Sommer, 2008).

Transparency

A question that arises is whether the forensic scientist actually has access to the artifact data and technology. If not, they might look at it as a 'black box', but the essential issue is the validation of the information extracted from the system. In many cases trade secrets are a hindering factor. Open source projects in general give more insight into the technology that is used, however source code review is a labour-intensive task.

Disclosure

With many proprietary systems it is not known if there are 'back doors' in the software, which allow the manufacturer (and thus anyone else who becomes aware of it) to circumvent the protection system. However, not everything can be disclosed in a court room, since manufacturers also sometimes have non-disclosure agreements with the expert. The reason is that they do not want to share methods with the public, or that the government would not like to disclose a certain method, since then it will not be useful in future cases.

How Long Is Data Kept?

To examine data, it is important to know how long the data is kept. Camera surveillance systems are known to typically keep their data for several days, after which they will overwrite it. These kinds of issues have to be taken into consideration. In some cases additional information can be extracted from data caching or other areas where the information was temporarily stored.

Legal and Ethical Issues

A forensic scientist should also know the rules relating to data protection legislation. Often in criminal law the system can be examined. However, whether it is admissible in court depends on the laws of the country and how the information was gathered. For example, in the Netherlands wiretaps are commonly used as evidence in court, whereas in the United Kingdom this is not admissible, which is based on the ethics within a law system. Other ethical issues one should be aware of are, for example, that personal details may become available from the data that is extracted.

Unintended Audit Trail

Unintended aspects are those of the artifact or the means of using it which yield information of forensic value. In some cases useful information such as GSM location data can be extracted. Using this data for locating someone goes beyond the original purpose of the network provider storing this information, which was for billing purposes.

8.3.2 Example 1: Mobile Networks[19]

Information from mobile networks is currently used as evidence in court. The determination of a location of a mobile phone is important to check if a person has been at a certain place and time. This can also be used to check information from witnesses and from the suspects. Furthermore, information who is calling who and SMS-details can be used as evidence in court.

However, one should always consider that the real identity of the user is not necessarily the person who is the subscriber or the purchaser of a prepaid phone, since the phone may be stolen or borrowed. A further problem is that certain models of SIM-cards can be cloned. Beyond these and other technical issues, on a management level the reliability of collected data may be undermined by fraudulent employees or contractors, software faults and other such issues. As such, although there is valuable data that can be exploited, the integrity of such data must be carefully considered.

8.3.3 Example 2: Biometric Devices[20]

Concluding from research in FIDIS deliverable 6.1, it is evident that the current state of the art of biometric devices leaves much to be desired. A major deficit in the security that the devices offer is the absence of effective liveness detection (Figure 8.4). At this time, the devices tested require human supervision to be sure that no fake biometric is used to pass the system. This, however, negates some of the benefits these technologies potentially offer, such as high-throughput automated access control and remote authentication.

The independent testing of biometric devices is still non-trivial as manufacturers tend to sell their products for more than they can achieve. The latter can give a false sense of security, adversely affecting actual security if not recognized in time. It is an issue that we encounter in many forms of technology today: if it can be cracked, it will be cracked. Accepting this would need a different attitude of manufacturers, in which more of what is going on inside the device and the accompanying software is made public. It would allow potential users of biometric systems to better judge the fitness of such systems for their particular purposes.

From a forensic point of view, care should be taken when drawing conclusions from information extracted from access control systems that use biometric devices. The possibility that the system was compromised, consequently falsely linking persons to events, should be examined or at least noted in the forensic examination report.

---

[19] Based on FIDIS deliverable D6.1 (contribution by Falk Wagner).

[20] Based on FIDIS deliverable D6.1 (contribution by Rikkert Zoun).

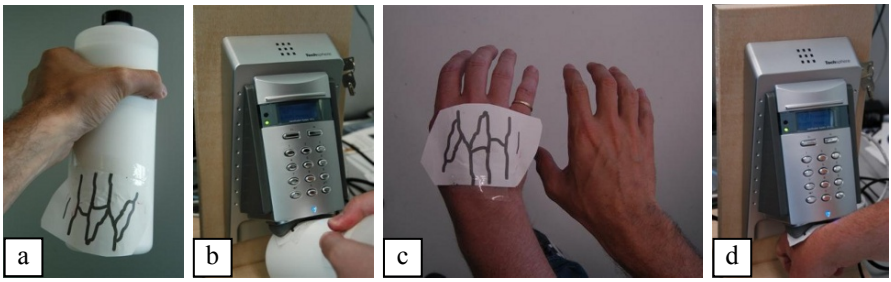

Fig. 8.4. Vascular pattern spoofs effective with liveness detection turned off. a) The copy of a vascular pattern stuck on a bottle. b) The bottle spoof verified as an authorized user. c) The copy of a vascular pattern stuck on a hand (left), next to the original hand (right) of an authorized user. d) The hand spoof verified as the authorized

8.3.4 Conclusion

This work has been an overview of issues that arise from different perspectives of Identity Management Systems and their forensic implications. As has been shown, information from digital systems can be useful as evidence in the court, however it is important to be aware that identities can be stolen or 'borrowed' in the case of a mobile device, and devices such as biometric systems do not always function as expected for technical, management or other reasons.

Although the information that is extracted from such systems can be used as evidence in court, for forensic science, it is important to give a statement of the technologies limitations and thus how strong or weak the evidence alone is. As such, it is important to also consider other available evidence. With many systems there exists a possibility of incorrect association of a user with a mobile device, deliberate tampering with the system or system error through incorrect usage or technical faults. A classic example is that fingerprints can be spoofed, and indeed other biometric features can be copied, even without the owner of that feature knowing it. Additionally, the claims from the manufacturers of the devices should always be verified. If they claim a device has liveness detection for example, this should be checked. For these reasons, in the examination process, it is important to consider the likely integrity of the data, i.e., how failsafe the system is, since this could provide an alternative hypothesis such as a different individual being involved in the crime. Equally, it is necessary to ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

8.4 Forensic Profiling[21]

8.4.1 Introduction

In the context of crime or criminal investigation, profiling is often assimilated with offender profiling, psychological profiling or the use of investigative psychology, mostly, although not exclusively, in the context of violent crimes. DNA-profiling is a different term that is also familiar to a wide range of the population even if its exact scope remains largely unknown. Another immediate perception of profiling in a forensic context is the application of data mining techniques to an important quantity of data collected from crimes and persons in order to recognize patterns that may inform about illegal activities. Less known, but the object of growing interest, is the field of illicit drug profiling (systematic extraction and storage of chemical attributes of drugs seized in order to obtain indications on the manufacture and distribution processes, the size and the evolution of the market). There is thus no one single use of the term "profiling" in forensic science and intuitive meanings apparently lead to very different territories. If the psychological viewpoint appears to fascinate and attract many people, DNA, illicit drug profiling and data mining dimensions appear to belong to technical and highly specialized fields, largely inaccessible to the public.

The distorted perception of all of the dimensions that lead to wrong expectations and fears: common sense vision of forensic science and criminal investigation differs considerably from concrete practice. Moreover, many different communities of researchers participate in the debate by developing similar but loosely connected models and approaches. These are based on different bodies of knowledge mainly borrowed from psychology, sociology, criminology, forensic science, crime analysis and criminal intelligence, or statistic and computer science. Finally, what really works and what does not is not easy to distinguish.

Thus, in the perspective of the FIDIS project, the process of balancing risks for the subjects and opportunities for the data controller is not easy (Hildebrandt and Gutwirth, 2008). For instance, weighing up the risks of being wrongly profiled as a criminal in the course of an investigation, and the opportunity for investigators, law enforcement agencies or the criminal justice system to be able to neutralize dangerous criminals early, is not straightforward. There is an initial need to find some unity within these scattered pieces of works.

A better definition of the term 'forensic profiling' is also essential from a forensic perspective because notions of identity and identification are at the core of the domain and should properly integrate evolutions associated to identification systems and new identities in the information society. Moreover, forensic science needs new frameworks in order to make the best use of data mining technology, not only in the treatment of electronic traces, but also to exploit more traditional forensic case data. This convergence between the different fields of forensic science, and particularly what is called forensic Information Technology (forensic

[21] Based on FIDIS deliverable D6.7c (contribution by Geradts/Sommer/Ribaux).

IT), with methods for their exploitation such as data mining, seem to constitute one of the biggest challenges for the future.

This is a considerable task, as forensic science is too often considered to be a list of separated and narrow specialties. However, this FIDIS task, connected with results obtained from other FIDIS activities, offers an opportunity to take some steps towards this objective.

Thus, the distinctions that are provided here aim to identify some of the profiling-related concepts, inferences and technical methods explicitly or tacitly used, as the object of research or applied in practice. Reasoning activities that may be assimilated with profiling are pervasive. Of these inference forms, some are identified here as an element of a more global approach of profiling (Hildebrandt and Gutwirth, 2008). This account is not intended to be comprehensive, because relevant dimensions go far beyond what can be explored in the single task of this project.

8.4.2 Definition of Forensic Profiling

We consider that forensic profiling consists of the exploitation of traces in order to draw profiles that must be relevant to the context of supporting various security tasks, mostly in the criminal justice system. A distinction of forms of profiles that are used in this context is necessary before evaluating applications of data mining techniques for forensic profiling.

8.4.3 Linkage Blindness and Limits of Profiling

It may be perceived that the necessary data for forensic profiling is immediately available in a suitable form to the criminal justice system. This is definitely not so. Methods for processing data carefully distinguish a selective collection of traces, the collation of the data coming from different sources, the evaluation of its quality, the analysis of the available information and the timely dissemination of intelligence or knowledge on a need-to-know and right-to-know basis (Peterson et al., 2000). This decomposition helps to make explicit a series of pervasive difficulties when profiling is envisaged.

A broad variety of barriers that go far beyond the inadequate use of technologies (Sheptycki, 2004) hamper the fluidity of information. These can lead to a well identified weakness called linkage blindness (Egger, 1984), an obstacle to the detection of relevant patterns in the information which exist in reality. This incapacity to connect the dots is generally accepted to be at the origin of main intelligence failures (United States, 2004). Below are some examples of causes, but other legal, organizational, methodological, technological, human and fundamental (complexity) causes may also lead to linkage blindness.

- Law enforcement data is scattered into different files and in different jurisdictions. For instance DNA and Automatic Fingerprint Identification Systems (AFIS) may be centralized at country level, but both databases are generally treated separately as the result of legal rules. Moreover, databases

may also use different classification systems and even preclude extractions of parts of the data, as well as electronic exchanges.

- Beyond police recorded data, administrative data and openly accessible sources, information is generally not directly accessible and available. If we suppose a specific situation, a judicial authority must intervene to authorize the access by the police and to order the possessor to grant access. This may dramatically slow down the whole process. Consequently, this may invalidate the analysis of the data in regard of of the dynamics of the problem under scrutiny. For example, several months are sometimes needed for obtaining some set of data in the framework of international cooperation agreements.
- Data comes from multiple sources under a broad variety of forms, which can still occasionally be a paper form. Moreover, the whole data treated, even police recorded data, is not prepared for profiling purposes, rather, it is structured for strictly administrative purposes.
- Profiles are hypotheses that are based mainly on imperfect (incomplete and uncertain) information. Thus, profiles may provide irrelevant leads and recovery from wrong investigative directions must be possible through recording assessment of the solidity of the information upon which hypotheses have been drawn.

These difficulties are obstacles to the treatment of data. Whether or not data mining technologies are implemented is not an essential question here. Rather, it appears that collection of data, evaluation of the information and the pre-processing stages for collating different sources of information generally imply a significant effort that must absolutely precede analysis and profiling.

This is particularly evident when dealing with the more fundamental questions of devising models in order to collate data coming from scattered sources. This data is generally available in different formats and must be structured in a suitable form for analysis purposes. Generally, at least three main dimensions of analysis appear relevant when dealing with criminal data for analysis purposes: what are the entities (for instance objects, individual, groups, traces, series, incidents, etc.) and their relations (for instance this person own this car), chronologies (for instance sequence of transactions between bank accounts), and spatio / temporal developments (for instance concentration of activities and their evolutions). It is very doubtful that data mining would be possible without first engaging efforts to collate the data. This is done through models that are based on at least one of those dimensions, depending on what the problem at hand is and what is searched for in the data.

Finally, disseminating obtained results in order to make intelligence products available to an organization is a critical aspect of the whole methodology. The quality of communication influences the possibility to appropriately use the obtained profiles in the field. The analytical part that entices profiling, at the core of the process, must thus be carefully considered within a broader process.

8.4.4 Data Available

Roughly speaking, sets of data available to law enforcement agencies are divided into two categories:

- Nominal data directly designates persons or objects (recidivists, intelligence files and suspect files, stolen vehicles or objects, etc.) and their relations. Nominal data may also be obtained in the framework of specific investigations, for instance a list of calls made with a mobile phone (card and / or phone) that cover a certain period of time, a list of people corresponding to a certain profile, or data obtained through surveillance.
- Crime data consist of traces that result from criminal activities: physical traces, other information collected at the scene, from witness or victims or some electronic traces, as well as reconstructed descriptions of cases (*modus operandi*, time intervals, duration and place) and their relations (links between cases, series).

Nominal data and relations may be abstracted in order to describe the structure of groups of offenders or criminal organizations.

Crime data are ideally also regrouped into abstract descriptions according to recurrent situations that share typical mechanisms. For instance, credit card frauds may be distributed into classes that separate skimming, distraction thefts, other thefts, etc. However, most of the time, data is initially administratively classified according to legal definitions which may mask the real dynamic behind crime problems (Goldstein, 1990). This emphasizes the necessity to make a distinction between sources of traces (persons or objects), the activity or situation that may explain the traces (the dynamic of the crime: context, immediate environment, victims, offenders) and the offense (legal definition) (Cook et al., 1998; Jackson et al., 2006).

The difference between crime-data and criminal data through crime / criminal data has led to a distinction between the fields of crime analysis, mostly carried out at a regional or local level, and criminal intelligence analysis, mostly the province of central agencies. This duality usually designates two professional communities (Bruce et al., 2004)[22]. However, both are obviously linked under many forms, particularly because traces directly result from behaviours of individuals and help provide some kind of description. This is compound by the aim of the investigation to identify, localize, and then provide evidence about the link between a trace and a person, to assume an activity or help determine an offense. In this context, forensic profiling will constitute the process that focuses on the exploitation of traces, but may overlap with criminal intelligence analysis.

[22] IALEIA: International Association of Law Enforcement Intelligence Analysts; IACA: International Association of Crime Analysts.

8.4.5 Structuring Evidence and Profiling

When a suspect has been arrested, forensic scientists may advise an authority on how to deal with traces and provide leads on new traces to be collected. At this stage, a lot of activity is dedicated to test the consistency of available information, under the assumption that the suspect is at the source of the traces and the activity. A test of consistency with the hypotheses is not sufficient for going to court (see above), but it may lead to refute the hypotheses if available traces show unexplained discrepancies.

For instance a person who is supposed to have used her credit card at one place could not have used simultaneously her mobile phone at another distant place. In terms of profiles, coherence of the profile of the person under scrutiny has to be tested from various perspectives in order to detect potential contradictions or on the other hand to support hypotheses by demonstrating consistence (it has still to be confirmed how those concordances may occur by coincidence!). For instance, it may be assumed that the use of a mobile phone is part of the modus operandi of a serial offender when he is operating. Thus, data related to the localization of mobile phones should show spatio-temporal coherence with data related to the crimes themselves. Correlation between different sources of data (traces) may be thus intensively used according to the hypothesis to be tested.

8.4.6 Forensic Profiling in an Investigative Perspective

As stated by many authors (Kind, 1987; Wiggett et al., 2003; Jackson, 2004; Jackson et al., 2006; Mennell, 2006; Mennell and Shaw, 2006), there is the realization among forensic scientists that their role must extend to the investigation itself. They must be particularly engaged when hypotheses have still not been entirely drawn, in the coordination of the forensic information collected, as well as for proposing new collection of data. In this way, the forensic scientist turns from an evaluator to a more investigative attitude (Jackson et al., 2006): who / what is the source of this trace, how can we explain the existence of these traces, what is the offence, what evidence may indicate some possibilities for new data collection, what support and leads to the investigation may be provided, where is the person who committed the crime, etc.?

This contribution is based on an entirely different inferential process than for interpreting evidence for the court. Rather than balancing probabilities related to given propositions, it focuses on the development of alternative hypotheses that may explain the existence of traces. Thus, rather than testing the hypothesis of culpability or innocence, we could generally describe the process as starting from the effects (the traces) and imagining possible causes on the basis of general knowledge (abduction and induction). Forms of profiling that arise during the investigative part of the process are manifolds and combine individual profiling with group profiling (Jaquet-Chiffelle, 2008). We do not have the pretension of identifying all the possible forms here, only the most typical will be described.

One of the basic operations consists of creating a first profile from the available (collected) information and then searching for all the persons or their relations to objects that correspond to this profile. Profiles are described here as categories that restrict the search within a 'selected' population. A person (individual) may generally be described through traces:

- They themselves reflect directly some physical aspects of the sources and have some descriptive capacity, such as fingermarks or DNA profiles extracted from biological marks, a snapshot taken from a camera.
- Traces and where they are found may be used to infer some indications about physical aspects or inform about clothes or accessories: earmarks found at a certain height on a door and the size of shoemarks may indicate (qualitatively) how tall the source is; a snapshot may provide some physical description as well as information about clothes and accessories.
- Traces may indicate the make and model of the printer used to print a recovered document, a bullet collected at the scene of crime may indicate the make and model of the firearm used, while paint marks coming from a car may point to a make and model of the implicated car. These are all types of acquisitions that may indirectly point to a person. Other possibilities include the use of fibre for inferring description of clothes, toolmarks or other marks for obtaining some description of the tools used. In a similar way of thinking, but about persons, DNA profiles indicate the gender (generally not more about the physical aspect through non-coding DNA sequences chosen for forensic use).
- The activity and behaviour in the immediate environment may be inferred through a global analysis of the spatial (and temporal) distribution of traces, such as a sequence of shoemarks, a sequence of withdrawals with a specific bank card at different ATMs, traces of navigation with an internet browser.
- Circumstances and application of different theories from different bodies of knowledge may help to interpret the situations in order to provide other traits of the person or of his behaviour. For instance, geographical profiling (mostly for serial crimes) aims at providing clues for localizing a person (Rossmo, 1999), or different theories point out that psychological traits may also be inferred. The person may also be the object of a classification process into different categories (pre-defined classification of computer crime offenders, arson offenders, rapists, etc.).

Each final profile may thus be more or less general. Its attributes are known or unknown, complete or not and mostly uncertain.

One of the main (but not the only) questions of the investigation is the identification of the sources of the traces and how they may be related with the activity. Developing hypotheses about who / what is the source may be straightforward for

instance through the use of DNA databases or Automatic Fingerprint Identification Systems (AFIS). Those systems start from the traces that come from a source (data subject as defined in Hildebrandt, 2008a), transform them into a digital form (attribute of a virtual person (Jaquet-Chiffelle, 2008)), compare them with collections of reference material and suggest as output a (list of) possible candidate(s) (or list of virtual persons) that refer to possible data subjects. The result is then interpreted and integrated into the investigation process. When using AFIS databases, a list of candidates is returned by the system, while for DNA databases, usually a single profile[23] is returned. However, with the evolving content of databases and since identical twins have the same DNA, occasionally several DNA-profiles may be returned by the database. Moreover, with the extended use of partial DNA or mixtures, putative sources may be multiple.

In order to generalize this process, a useful concept has been stressed by Kind (1987). He argues for the use of the dual concepts of frame and form. The frame contains the set of entities considered as relevant for the investigation, according to available evidence, while, roughly, the form distinguishes different region of the frame as more or less promising. A list of candidates extracted from an AFIS system constitutes the frame, while scrutinizing the content provides as outcome the form. The frame is often constituted of persons or entities that share a common profile. This may also be seen as a non-distributive group profiling approach (Hildebrandt and Backhouse, 2005; Hildebrandt, 2008b; Jaquet-Chiffelle, 2008) where a category of individuals is built on the basis of a different set of data and where the decision to insert an individual (or its individual profile) into the frame may depend on features of different natures.

There are many ways to develop a frame in the course of the investigation, depending on the case and available traces. The direct and simplest way consists in comparing the trace with the collection of reference material (like for DNA or AFIS databases). A similar process consists of comparing images taken from video surveillance systems (CCTV) with collection of photos taken from known persons. The scheme is the same and simple, but obviously the source of data used presents specificities that make the methods routinely applicable, as well as automated profiling possible or not.

Another possibility, when recidivism is known as frequent, is to compare the assumed modus operandi of the offender with the modus operandi used by known recidivists. Here again, when serial crime is considered, a profile extracted from the series of modus operandi used by the recidivist (a profile extracted from an already constituted set of information – individual profile) may be used to proceed to the comparison: the burglar usually operated during the night, entered the prem-

[23] The use of profile for DNA may be confusing in the context of this deliverable. However, a DNA profile may be defined as a description of a person through part of her DNA structures. Even if the parts of the DNA structure used in a forensic context have been chosen for their polymorphism across the population, the same profile may apply to several persons. A profile thus does not define a single individual, but rather a group.

ises through an open window, and generally selected only credit cards. There may be very different approaches for building such a profile, for instance by expecting that a specific feature occurs in each case or only in the majority of cases, expecting the existence of a specific feature of not, etc. The relevancy of such a profile depends on the expected use of the profile (searching other databases for linking cases, organizing specific surveillance, trying to intercept the perpetrators) and thus may take the status of intelligence (see below).

Another important form of profiling is carried out through the application of models and methods used for hypothesizing the place where the offender resides, or one of his centers of interest. These methods are known as geographical profiling and may be used in specific situations, for instance when or where a serial offender operates (Rossmo, 1999). With the development of new technologies, data extracted from GSM operators may play an important role in this perspective, for instance by assuming the degree of mobility of a person, where he resides or other spatial dimensions related to his behaviour.

Finally, other possibilities are developed through new id-systems: when a profile of the offender has been developed and some of his activities may be inferred, new frames may be built. For instance if the author was suspected of having used her mobile phone when operating, details of all the calls made during the time of the offense in the region of interest may be requested from the operator, with the hope of detecting the card or the mobile phone used by the offender. If an offender is supposed to have entered a building controlled through id-systems, the list of persons who entered the building may be provided.

All these forms may be used in combination through cross-referencing, for instance when geographical profiles lead to a list of inhabitants, the use of firearms may indicate the relevancy to search among the list of legal possessors, the profile of a car to consider the file of car owners, etc. This data may then be cross-referenced either to build a category of persons corresponding the best to the offender profile, conscious of the fact that the offender may or not appear in these databases. This may, as an outcome, provide a list of relevant identities to be further investigated.

Jaquet-Chiffelle (2008) stressed that this kind of investigative profiling follows two distinct goals: the first is to identify an individual within a community or infer its habits, behaviour, preferences, knowledge, etc. But the second form is not independent from the first one as it is often not obvious, once identified, to find (ultimately arrest) a person worth being the object of further investigations. Occasionally, the localization of the person even leads to his arrest before he is identified. For instance, when a serial burglar operates, his pattern may be detected and used to devise surveillances that may in turn lead to his arrest.

A rich example, well documented, of possibilities for applying such techniques can be found in the review of the investigation of the Yorkshire Ripper during the 1970s (Byford, 1981). This investigation offers a broad series of inferences and treatment of data typical of complex investigations. Review of the case has led to an overview of profiling (Kind, 1987). At that time, among other difficulties, the lack of computerization and possibilities of cross referencing was identified as a

severe handicap for the investigation. The ripper was finally arrested through a routine control in the street, because he was circulating with stolen plates. Despite that this arrest was made in isolation from the investigative strategy itself, it was actually also obtained through the use of a systematic control process aided by the databases of stolen plates. Lessons learned from this case have had in particular considerable impact on the development of computerization for major case management[24] and organizations of incident rooms. It may also be considered as a milestone in the development of analytical capabilities within law enforcement such as geographical profiling or the use of information technologies in the management of serious cases.

8.4.7 Illicit Drug Profiling

The systematic chemical and physical analysis of illicit drugs seized by law enforcement agencies has greatly developed since the middle of the 1990s (Guéniat and Esseiva, 2005; Ioset et al., 2005). Illicit substances are seized, transferred to laboratories, and analyzed in order to extract a profile (list of chemical substances and their quantities). The profiles are then recorded into a database which is exploited in an intelligence or investigative perspective. For instance the process of linking illicit substance seized in different circumstances may lead to concentrate attention to a specific organized network while they were previously the object of separated investigations. Other indications about cultivation (origin), manufacture processes, or the distribution process of illicit drug trades can be inferred through the systematic analysis of the database.

The data is organized into a dynamic memory: seizures are not stored individually but are rather collated and grouped into classes mainly according to similarity measurements between profiles coming from different seizures (Dujourdy et al., 2003; Esseiva et al., 2003). Depending on which basis they are formed, these clusters mainly indicate similarities in the traffic at different levels, from the cultivation (origin) to the distribution of the illicit substance.

Beyond standard clustering methods, other original methods for detecting patterns have been tested, particularly through spatio / temporal and graph visualizations. For instance, combinations of cutting agents are often used by drug smugglers before distribution on the street. The spatio / temporal evolution of these co-occurrences inform on the dynamics of the local market (Terrettaz-Zufferey et al., 2007).

However, there is evidence that each drug trafficking network and laboratory develop its own recipes and methods that reflect differently into the intrinsic structure of the chemical profiles (correlations between variables). Thus, there is no suitable universal metric that can be defined, except for those specificities, that can systematically provide the same reliability when measuring proximity between samples. There is a need for a typical learning process as classes or specific

[24] Development of the HOLMES system (Home Office Large Major Enquiry System).

groups profiles evolve over time, and show an inherent structure that may in turn influence the classification of new data.

This hypothesis has been tested with data coming from known solved cases. Spectral clustering and its variants have been chosen to train the system and have shown to substantially improve the classification process (Ratle et al., 2007). How those ideas may lead to the development of unsupervised methods is now the subject of further developments.

However, even if comprehensive European projects have led to some harmonization and extension of the use of the method, in particular in the field of amphetamines (Aalberg et al., 2007a; Aalberg et al., 2007b; Andersson et al., 2007b; Andersson et al., 2007a; Andersson et al., 2007c; Lock et al., 2007), we are far from exploiting the whole potential of the approach. In fact, the central question is how to integrate knowledge extracted from drug profiling databases with the analysis of other (traditional) sources of information (geopolitical, coming from investigations, etc.). Full aggregation of data, even theoretically ideal, can now be difficult to imagine as organizations that deal with the set of data are different (mostly forensic laboratories and the police), cover different countries and are based on different specialties. A more pragmatic model consists in the development of communication channels between partners organized as a network. For instance, chemical links can be systematically provided to the police and used in the investigative process. Conversely, investigative hypotheses can be tested through chemical profiling (Ioset et al., 2005). This integration process must attract much more attention than the lack of communication between the organizations (police, forensic laboratories and Universities) actually allows in practice.

8.4.8 Legal Aspects[25]

Profiling in forensic science is still inchoate as we can see from the examples, although there is much research in this area. As with searches in databases, one should be aware of false interpretations of hits. False hits can be caused by the size of the database, by the techniques used, and since databases are often not very 'clean'. The persons that interpret the information from profiling should be very aware of the limitations of the methods. In the example of the camera surveillance, one should be aware that artifacts which are used for identification can also be changed. This should always be considered in forensic evidence, and should be included in the chain of evidence.

New ID systems with strengths to detect what was previously impossible, but weaknesses when they provide false positives, still offer new opportunities for improving and consolidating security. Indeed, electronic traces are information among others that are valuable in the context of the criminal justice system and forensic science.

[25] Based on FIDIS deliverable D6.7c (contribution by De Vries and Coudert).

In the light of new technological advances in the field of forensic profiling, i.e., the interconnectivity databases and risk profiling, the existing data protection instruments are not always effective anymore. As commissioner Frattini recalled 'the protection of fundamental human rights such as privacy and data protection stands side-by-side with public safety and security. This situation is not static. It changes, and both values are able to progress in step with technological advances. But it also means that there must be lines which cannot be crossed, to protect people's privacy' (Franco Frattini, 20 November 2007). However, as pointed out by the European Data Protection Supervisor, the different instruments adopted at European level 'have in common that they enable a global monitoring of movements of individuals, even if from different perspectives. The way in which they can already contribute to the fight against forms of crimes, including terrorism, should be subject to in-depth and comprehensive analysis.'[26]

In that sense, the European Parliament pointed out that 'Governments and EU institutions have often responded to terrorist attacks by adopting laws that have not been sufficiently discussed and sometimes in violation of basic human rights such as right to privacy or to a fair trial. Members call for further scrutiny of intelligence operations and for more proportionate and evidence-based legislation in the future.'

In fact, the different norms approved at European level remain insufficient as they do not deal with the fundamental issues at stake before the widespread use of criminal intelligence, the increased monitoring of the average citizen or the increased linkage of police databases. Such instruments, fruit of difficult political consensus, implement principles broadly formulated and containing important derogations to the general data protection principles. Significant issues such as how to ensure the transparency and accountability of law enforcement activities, the quality of the data processed, e.g., the differentiation between categories of data subjects, or a strict application of the purpose specification principle remain unanswered. Moreover the comments of the European Commission, the European Data Protection Supervisor and the European Parliament are often not taken into account. At the level of the Council of Europe, the data protection principles formulated in the 1980s remain broad and subject to interpretation by Member countries.

Another complication is that the multitude of initiative creates a complex framework prone to legal loopholes and difficult to comprehend. The draft Framework decision on data protection in the third pillar has been limited to the exchange of personal data between law enforcement authorities and fails to provide the third pillar with a comprehensive and strong data protection framework. Furthermore, the European Data Protection Supervisor stressed that for certain aspects the current text of the proposal does not provide for the same level of protection as defined in Convention 108. This certainly seems to be the case with the

[26] European Parliament resolution of 12 December 2007 on the fight against terrorism, B6-0514/2007, available via http://www.europarl.europa.eu/.

provision on the further use of data received from a Member State (Articles 3 and 12) and the right of access (Article 17).[27]

All these factors create legal uncertainty and should lead each Member State to face individually the challenges of ensuring that the new activities developed within the law enforcement field are subject to the principles of 'scrutiny', 'accountability' and 'transparency', in a context of increased international activity and exchanges of criminal data. Each country will thus be called to make the specific balance between the competing interests at stake, in particular to prevent that the increasing use of personal data for risk prediction turns into stigmatization of parts of the population.

It is, however, too soon to evaluate how the European Commission will implement the required safeguards and balance the different needs at stake. It suffices to say that the proposal for a Framework Decision for data protection in the third pillar constitutes a first laboratory where the aforementioned safeguards will have to be implemented.

8.5 Conclusion

In this chapter, we have focused on identity-related crime: the concepts and techniques involved, and the legal, organizational, and technical measures to combat crimes in which identity is used as a target or principal tool. We have also looked at the mirror image of identity-related crime: forensics implications. Identifying perpetrators is one of the key functions of forensics, and given the increasing importance of identity management in the information society, identity-related forensics is emerging as a major field of study. A particular application is forensic profiling, in which traces are used to draw profiles that are relevant to supporting various security tasks, most notably in the criminal justice system.

Our discussion shows that identity-related crime and its implications for forensics, as well as forensic profiling, thrive on technologies and procedures for identification, which have become increasingly varied and complex with the advent of the information society. Weaknesses in identification procedures that enable identity-related crime are equally relevant to be aware of in identity-related forensics, where evidence of who committed a crime or tort may crucially depend on linking traces of evidence to a specific individual. Particularly in a digital environment, establishing the link between identifiers and individual is far from easy. Detailed knowledge of the technologies involved is crucial, but not enough. Equally important are a good grasp of identification procedures, of the organizational context of identification measures, and of the legal context. Only through multidisciplinary

[27] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, *Official Journal* 23.6.2007, C139/1, available via http://www.edps.europa.eu.

research can we begin to understand the mechanisms that facilitate both identity-related crime and identity forensics for successful criminal investigation.

One of the lessons of five years of multidisciplinary FIDIS research is that it is useful to first establish a common ground for research: analyze concepts, definitions and taxonomies from different disciplinary perspectives, in order to come to a converging understanding of the key concepts at issue. Without such a common ground, no useful multidisciplinary debate can take place on policies or measures to address the complex problems that we face in the information society.

A second lesson, however, is that it is important also to move forward beyond concepts and definitions. The debate about identity-related crime sometimes seems to remain at the level of definitions, where the need is stressed for defining separate categories of identity-related crime before statistics on its prevalence can be collected. The implication is that policies cannot be devised without knowledge of how frequently which types of identity-related crimes are occurring. Criminals, however, are not interested in definitions – they simply use whichever vulnerabilities they can find to commit a crime, and when they find weaknesses in identification management systems, they will not hesitate to exploit them.

Therefore, for future research, rather than focus on generally accepted definitions, lack of data and whether or not to start registering identity-related crime before countermeasures can be taken, a better approach to address the threat of identity-related crime may well be to start conducting more in-depth studies of the strengths and weaknesses of European identification infrastructures in the information society. Based on such studies, timely and targeted measures can be taken by European governments, businesses, and citizens alike to effectively combat identity-related crime and to establish successful tools for identity-related forensics.

Reference

Aalberg, L., Andersson, K., Bertler, C., Borén, H., Cole, M. D., Dahlén, J., Finnon, Y., Huizer, H., Jalava, K., Kaa, E., Lock, E., Lopes, A., Poortman-Van der Meer, A., Sippola, E. (2007a), 'Development of a harmonised method for the profiling of amphetamines I. Synthesis of standards and compilation of analytical data', Forensic Science International 169: 219-229.

Aalberg, L., Andersson, K., Bertler, C., Borén, H., Cole, M. D., Finnon, Y., Huizer, H., Jalava, K., Kaa, E., Lock, E., Lopes, A., Poortman-Van der Meer, A., Sippola, E., Dahlén, J. (2007b), 'Development of a harmonised method for the profiling of amphetamines II. Stability of impurities in organic solvents', Forensic Science International 169: 231-241.

Aitken, C. C. G. and Taroni, F. (2004), Statistics and the Evaluation of Evidence for Forensic Scientists. John Wiley & Sons, London.

Anderson, D.S., Fleizach, C., Savage, S., Voelker, G. M. (2006), 'Spamscatter: Characterizing Internet Scam Hosting infrastructure', Proceedings of the USENIX Security Symposium, Boston, MA.

Buitelaar, H. (ed.) (2007), FIDIS Deliverable D13.3: Study on ID Number Policies, Download: www.fidis.net/resources/deliverables/.

Byford, L. (1981), 'The Yorkshire Ripper Case: Review of the Police Investigation of the Case', H.M.s.I.o. Constabulary, Home Office.

Cook, R., Evett, I. W., Jackson, G., Jones, P. J., Lambert, J. A. (1998), 'A hierarchy of propositions: deciding which level to address in casework',. Science & Justice 38: 103-111.

De Vries, U. R. M. T. et al. (2007), 'Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen', WODC, Utrecht, http://www.wodc.nl/images/1496_%20volledige_tekst_tcm44-86343.pdf.

Egger, S.A. (1984), 'A Working Definition of Serial Murder and the Reduction of Linkage Blindness', Journal of Police Science and Administration 12(3): 348-355.

Frattini, F. (2007), 'Closing speech on Public Security (20 November 2007)', Speech /07/ 728. Privacy and Technology Conference on Public Security, Privacy and Technology, Brussels.

Geradts, Z. and Sommer, P. (eds.) (2006), FIDIS Deliverable D6.1: Forensic Implications of Identity Management Systems, Download: www.fidis.net/resources/deliverables/.

Geradts, Z. and Sommer, P. (eds.) (2008), FIDIS Deliverable D6.7c: Forensic Profiling, Download: www.fidis.net/resources/deliverables/.

Goldstein, H. (1990), Problem Oriented Policing. Temple University Press, Philadelphia.

Grijpink, J. H. A. M. (2006), 'Identiteitsfraude en overheid', Justitiële verkenningen 32(7): 37-57.

Hildebrandt, M. (2008a), 'Defining profiling: a new type of knowledge?' In: Hildebrandt, M. and Gutwirth, S. (eds.), Profiling the European Citizen: Cross Disciplinary Perspectives. Springer, pp 39-50.

Hildebrandt, M. (2008b), 'Profiling and the Identity of the European Citizen'. In: Hildebrandt, M. and Gutwirth, S. (eds.), Profiling the European Citizen: Cross Disciplinary Perspectives. Springer, pp 320-360.

Ioset, S., Esseiva, P., Ribaux, O., Weyermann, C., Anglada, F., Lociciro, S., Hayoz, P., Baer, I., Gasté, L., Terrettaz-Zufferey, A. L., Delaporte, C., Margot, P. (2005), 'Establishment of an operational system for drug profiling: a Swiss experience', Bulletin of Narcotics 57 (1-2): 121-146.

Jaquet-Chiffelle, D. O. (2008), 'Reply: Direct and Indirect Profiling in the Light of Virtual Persons'. In: Hildebrandt, M. and Gutwirth, S. (eds.), Profiling the European Citizen: Cross Disciplinary Perspectives. Springer, pp 55-63.

Kind, S. S. (1987), The Scientific Investigation of Crime. Forensic Science Services Ltd, Harrogate.

Kind, S. S. (1994), 'Crime investigation and the criminal trial: a three chapter paradigm of evidence', Journal of the Forensic Science Society 34(3): 155-164.

Koops, B.-J. (2005), FIDIS Deliverable D5.1: A survey on legislation on ID theft in the EU and a number of other countries, Download: www.fidis.net/resources/deliverables/.

Koops, B.-J. and Leenes, R. E. (2006), 'ID Theft, ID Fraud and/or ID-related Crime. Definitions matter', Datenschutz und Datensicherheit (9): 553-556.

Koops, B.-J. et al. (2009), 'A typology of identity-related crime: conceptual, technical, and legal issues', Information Communication & Society 12(1): 1-24.

Kosta, E., Coudert, F., Dumortier, J. (2007), 'Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive', International Review of Law, Computers and Technology 21: 343-358.

Leenes, R. E. (ed.) (2006), FIDIS Deliverable D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, Download: www.fidis.net/resources/deliverables/.

Peterson, M., Morehouse, B., Wright, R. (2000), 'Intelligence 2000: Revising the Basic Elements'. Law Enforcement Intelligence Unit (L.E.I.U.) et International Association of Law Enforcement Intelligence Analysts (IALEIA), Sacramento, Lawrenceville.

Pintér, R. (ed.) (2007), FIDIS Deliverable D5.2c: Identity related crime in the world of films, Download: www.fidis.net/resources/deliverables/.

Rossmo, K. (1999) Geographical Profiling. CRC Press.

Sheptycki, J. (2004), 'Organizational Pathologies in Police Intelligence: Some Contributions to the Lexicon of Intelligence-led Policing', European Journal of Criminology 1(3): 307-332.

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

Terrettaz-Zufferey, A.-L., Ratle, F., Ribaux, O., Esseiva, P., Khanevski, M. (2007), 'Pattern Detection in Forensic Case Data Using Graph-Theory: Application to Heroin Cutting Agents', Forensic Science International 167: 242-246.

United States (2004) The 9/11 Commission Report, National Commission on Terrorist Attacks, http://govinfo.library.unt.edu/911/report/index.htm.

Van der Meulen, N. and Koops, B.-J. (eds.) (2008), FIDIS Deliverable D12.7: Identity-related Crime in Europe – Big Problem or Big Hype?, Download: www.fidis.net/resources/deliverables/.