OUR EMERGING INFORMATION SOCIETY

THE CHALLENGE OF LARGE-SCALE INFORMATION EXCHANGE IN THE CONSTITUTIONAL STATE

Inaugural address,

delivered on the occasion of the public acceptance of
an endowed chair at the Faculty of Mathematics and Computer
Science of Utrecht University, also for the Faculty of Law,
to work within the discipline of Information Science,
and more specifically *Chain-computerisation in the constitutional
state*

on 19 January 2005

by

dr mr J.H.A.M. Grijpink

Prof. Dr. mr J.H.A.M. Grijpink (1946) studied Economics (1969) and Law (1971) at Groningen University. He obtained his Ph.D. in 1997 at the Technical University Eindhoven for his thesis Chain-computerisation. He is Principal Advisor at the Strategy Development Department of the Dutch Ministry of Justice and is affiliated on a part-time basis to the faculty of Mathematics and Computer Science of Utrecht University as professor occupying an endowed chair, also for the faculty of Law. He is a Certified Management Consultant (CMC) and Registered Information Expert (RI).

His books Keteninformatisering ('Chain-computerisation') (1997), Werken met keteninformatisering ('Working with Chain-computerisation') (1999) and Informatiestrategie voor ketensamenwerking ('Information Strategy for Chain Cooperation') (2002) are published by Sdu.

Esteemed Chairman and Members of the University Board, Rector, Minister of Justice, Secretary-General of the Ministry of Justice, colleagues, family, friends and students, Ladies and Gentlemen,

It is a good custom in the academic world for a newly appointed professor to introduce himself in public and explain his field of study. I am pleased to take this opportunity to explain the new discipline of Chain-computerisation in the constitutional state and to indicate what I would like to bring about in partnership with colleagues and students during the next five years.

Chain issues

Barely a day goes by without chain issues making the news. Today's headlines are about football hooliganism, tomorrow's about juvenile crime or medical errors caused by faulty data transfer. Topical themes on the subject of chain cooperation include passport biometrics, the citizen service number and mounting identity fraud, for example. These issues always involve the large-scale exchange of information between huge numbers of independent organisations and professionals. They are often confronted with faulty cooperation or direct opposition, by suspects in the criminal law chain for example. If something goes systematically wrong with the communication in a chain, so many wrong decisions are taken that the chain becomes discredited. Our ability to tackle social problems is not keeping pace with the development of our society. In a social chain, no single party has the power to compel others to cooperate effectively. We are thus confronted with chain issues that are difficult to resolve. The computerisation of our society does however hold the promise of better-informed chain cooperation. But the gulf between what we are actually doing in the area of large-scale information exchange and what we need to do is getting bigger rather than smaller. In fact, we know precious little about how to bring about the exchange of information at such a huge scale, at least with sufficient guarantees of the data being used lawfully. The goal of my field of study 'Chain-

computerisation in the constitutional state' is to improve that situation. That is all the more important when we consider that the formation of the EU is leading to the internationalisation of many social chains, with all the complications that entails for the effective, lawful exchange of information.

Chain-computerisation

Our emerging information society increasingly calls for an approach of external communication that takes closer account of the needs and preconditions of chain cooperation. The large-scale exchange of data between autonomous organisations calls for a computerisation approach that is different from what we are used to. We must move away from treating large-scale communication systems as internal information systems with a somewhat larger group of users. It is for that reason that a distinct scientific basis with its own concepts, theories and methods is needed for the computerisation of social chains. That must give rise to new insights into the causes of the problems we are facing in the development of information infrastructures. In past years I have laid the foundation for tenets of that nature in my thesis and later publications, which have now been institutionalised in the form of an endowed chair entitled *Chain-computerisation in the constitutional state*. The social significance of these tenets is found in the notion that new insights can lead to better information strategies for our complex information society. That means more suitable information infrastructures for chain cooperation (covering the entire range from hard to soft infrastructure, from cables up to and including knowledge). Applying the chain-computerisation method makes it possible to distinguish promising chain projects from the rest, so that essential information infrastructures can be created more quickly. How can we otherwise structurally avoid a future situation in the travel chain in which somebody gets into difficulty in a foreign country because his identity has been misused? Or, without information infrastructures of that nature, how can we immediately establish in the criminal law chain of the future that the suspect is someone other

than who he has led the police to believe he is? Or that he is a habitual offender who needs to be tackled in a special way? Which chain communication do we need in the future to prevent new citizens from becoming isolated in Dutch society? There are countless other examples that could be given. In many social chains the number of misses, the so-called 'chain failure', is becoming an increasingly serious problem, further reinforced by our diminishing tolerance for poorly functioning social chains.

The 'chain' concept and the dominant chain problem

I have now used the word 'chain' a few times consecutively. By 'chain', I do not so much mean the logistics chain that we so often come across in the business community, but a social chain, such as social security, criminal law enforcement or treatment for drug addiction. Those are large-scale processes that yield a social product, such as income support, safety or survival. In a social chain of that nature many hundreds if not thousands of organisations work together without a clear relationship of authority in ever-changing combinations depending on the actual case. But cooperating with other organisations takes a lot of effort, time and money. There must therefore be a cast-iron reason for doing it. An important principle of our 'chain' concept is therefore that parties to a chain only cooperate if they are forced to do so by a dominant chain problem. A dominant chain problem is a problem that none of the parties can solve on his own. It is only by effectively cooperating that chain parties can prevent the systematic failure of their own organisation and the entire chain from being discredited. The identity chain, for example, cannot yet prevent your identity from being misused by someone else undetected. Identity fraud as a dominant chain problem in the identity chain forces parties to cooperate and determines the information infrastructure needed for that purpose, in which biometrics will play a central role in the future.

Chain thinking and chain laws

Ten years ago the concept of a 'chain' was still a vogue word without any practical significance. These days, we are more aware that each organisation must participate effectively in a large number of different chains. In practice, we find that it is difficult to reconcile the requirements of various chains. If an organisation acts both in the disaster recovery and the criminal law chain, should that organisation participate both in a chain with a person-based communication system (who is it about?) and in a chain with a geographically-based communication system (where is it?). That also serves to explain why many organisations have so much trouble with the structure of their internal information housekeeping.

Chain thinking is gaining in importance. Figure 1 briefly shows why. Advancing specialisation and mounting social requirements make organisations more and more dependent on each other. But chain cooperation proves to be anything but easy in practice. Because common interests are less pronounced than people think, and also often unclear, the cohesion that is so badly needed can only be provided by a serious dominant chain problem. Only then is there sufficient official and professional support for the large-scale exchange of information. Because of the absence of overall leadership, the chain proves to be a difficult administrative domain, in which processes like cooperation, decision-making and exchanging information proceed differently than *within* organisations. Rationality and expediency are hard often hard to find at the collective 'chain level', and unpredictability is the order of the day. If we leave aside the presupposition of rationality at chain level, we gain a clearer image of laws that play a predominant role at that level. Some of them are shown in figure 2.

Only a gradual approach, a modest measure or a selective system has any chance of success. The grander the envisaged solution, the less actual support there will be.

figure 1

> ## The importance of chain thinking
>
> - **chains becoming increasingly important:**
>   - advancing specialisation
>   - increasing mutual dependence
>   - mounting social demands
>   - increasing interaction and cooperation
> - **chains form a difficult domain:**
>   - absence of overall authority
>   - shared interests often limited and unclear
>   - irrationality and unpredictability hold winning cards at chain level
>   - the dominant chain problem 'rules' the chain!

figure 2

> ## Some chain laws
>
> 1. No amount of support is enough for a big solution; only a gradual approach is a feasible one
> 2. No interference with internal matters:
>   a. first computerise, then reorganise;
>   b. infrastructure: the 'emptier' the better
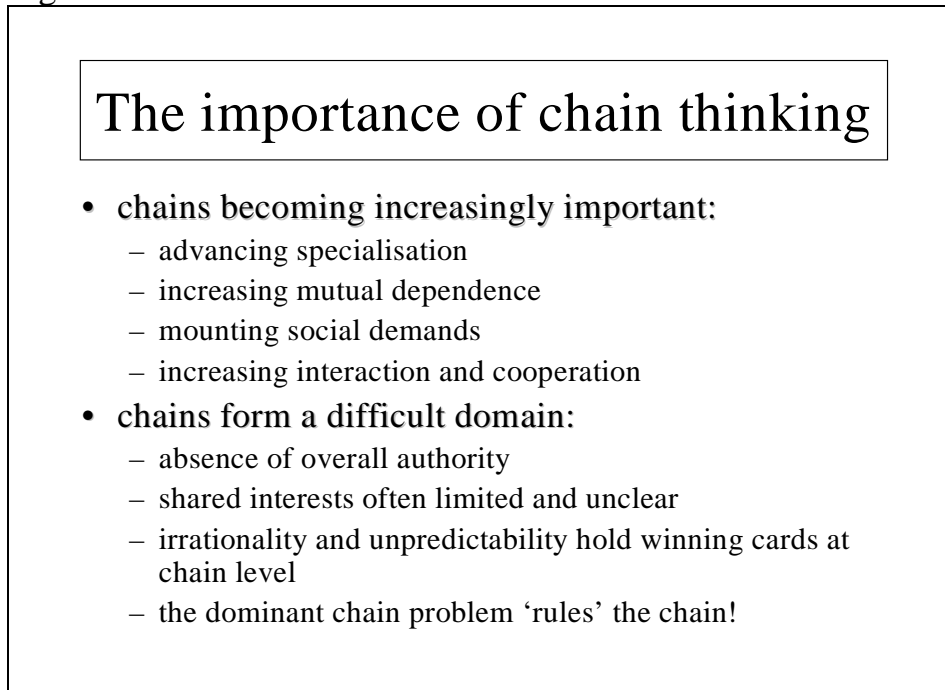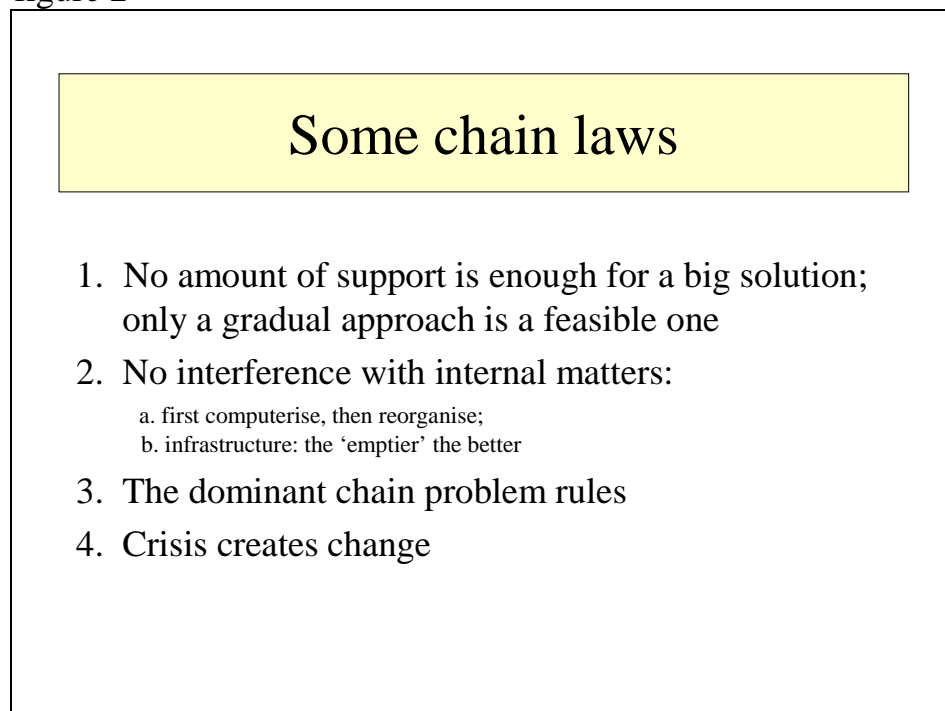> 3. The dominant chain problem rules
> 4. Crisis creates change

Measures at chain level that exert a strong outside influence on the internal affairs of chain partners come up against a lot of resis-

tance. We know this from the world of international diplomacy, but we rarely apply this insight to chain cooperation. It follows from the rule of 'mind your own business' that at chain level, unlike within organisations, computerisation of the essential communication has more chance of success than reorganising or integrating information systems. Large-scale change processes based on the power of persuasion and good intentions prove to be slow-moving and laborious. A crisis does however make changes at chain level possible, but we usually let that opportunity slip through our fingers because crisis management demands our attention. Put simply, chains form a bleak working environment. But that is nonetheless where the computerisation of society is to a significant extent taking place, with all the accompanying conesquences for the quality of life in the future information society.

Topical chain issue: a European criminal registry?
After these rather theoretical reflections, I now propose to apply this chain approach to a topical case in order to clarify the benefit of chain thinking. In July 2004 we were all shocked to learn of the case of Fourniret, the French serial killer who, after serving several long prison sentences, moved to Belgium and continued his murderous activities as the caretaker at a primary school. Apparently, his French criminal record had not been checked before he was given the job. Amidst the general outcry, a number of EU member states called for a central European criminal registry. The idea is that everybody would then know what's what. This is a common response to a social problem: set up a central register for each problem and that's that. In the mid-nineties in the Netherlands, for example, the Dutch Liberal party called for a central national database for sex crimes. At that time, too, the idea was warmly supported, both by the then Minister of Justice and by the civil service[1]. The downside of a central information system of that nature is that it is not possible to register and keep all relevant substantive

---

[1]   Quote: "VVD member Korthals […] presses for a national database for sex offences at the Central Criminal Information Department (CRI). The CRI itself has been calling for that for longer because the police cling too much to incidental cases", NRC Handelsblad, 22 August 1996, p. 3

information up-to-date on such a huge scale. Moreover, we often have too little time to check all sorts of databases in order to ascertain whether there is something we have to take into account in a concrete case. That is why central databases prove to be of little use in practice. Most projects of that nature get bogged down. And on the rare occasion that such an information system does get off the ground, it more often than not leads a stumbling existence.

But why *should* we expect anything of a central criminal registry for the European Union? After all, each EU country already has its own central registry of its own criminal convictions. The registration of convictions cannot therefore be the problem. Apparently, the problem is the exchange of that information across national borders. And perhaps even more: the cross-border use of information about convictions when making concrete decisions, such as when appointing a Frenchman as a caretaker at a Belgian school, or the Belgian judiciary's decision to rule out a Frenchman as a suspect for a Belgian crime.

So change is needed, but how? On 19 July 2004, the heading of NRC[2], a Dutch national newspaper, read: "Donner prefers the exchange of national information to a new European criminal registry". Indeed, why further centralise the storage of information about criminal convictions within the EU when what is most needed is better communication? In December 2004 the fifty (!) Ministers of Justice and Home Affairs of the European Union decided that all criminal convictions in the European Union would henceforth be referred directly to the Ministry of Justice of the convict's EU country of residence. A choice was made, then, to concentrate the criminal record of an EU citizen at the Ministry of Justice of the country of residence rather than to institute a central European criminal registry. Other EU countries can call up information about a person's criminal convictions in all twenty-five Member States in the convict's country of residence. According to

---

[2]   NRC Handelsblad, 19 July 2004, p. 1

this agreement, that information must be issued immediately, but within ten working days at the latest. This political agreement also provides for extension of the system at a later date to the exchange of information in the case of relocation. Does this solve the communication problem concerning conviction details? What stands out here is that the agreement in its current form leads to a better-organised way of registering criminal records. Why, then, should this agreement lead to better prospects for the cross-border use of information on criminal convictions when making concrete decisions? After all, in the Fourniret case, that is precisely where it went wrong, upon his appointment as a school caretaker. If the criminal record is not transferred in its entirety when someone relocates to a different country within the EU, we are still going to miss the boat when checking someone's criminal record for an appointment to a sensitive job position!
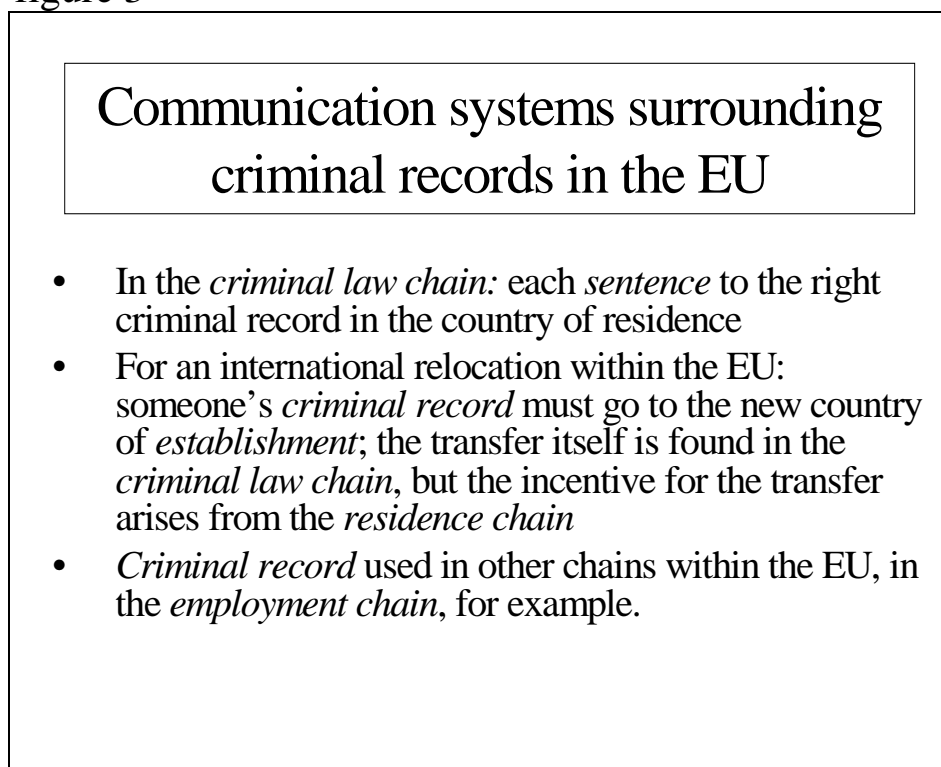
Now that the country of residence principle has been chosen for the criminal records in the EU, there are ultimately three hurdles to be taken for the chain communication involved:

1. a new *criminal conviction* in one of the twenty-five Member States must lead to an addition being made to the criminal record at the Ministry of Justice of the country of residence: this transfer of information about a conviction takes place within a single chain, the criminal law chain, but throughout the EU;

2. in the case of an international relocation within the EU, a person's *criminal record* must be transferred in its entirety to the Ministry of Justice of the new country of residence. Now two chains must communicate effectively to bring this about. The transfer takes place in the criminal law chain, but the incentive to transfer the record now arises from a different chain, which for the sake of convenience we will refer to here as the *residence chain*.

3. it must subsequently be possible for this transferred criminal record to be used in all EU countries when decisions such as

appointing someone as a school caretaker are made. Once again in a chain other than the criminal law chain, in this example the *employment chain*. For this communication the criminal law chain is to exchange information with a second chain depending the decision to be taken.

We thus see that the improved exchange of information concerning the national criminal records of the European Union calls for at least three different chain communication systems at EU scale (see figure 3).

figure 3

Communication systems surrounding criminal records in the EU

- In the *criminal law chain:* each *sentence* to the right criminal record in the country of residence
- For an international relocation within the EU: someone's *criminal record* must go to the new country of *establishment*; the transfer itself is found in the *criminal law chain*, but the incentive for the transfer arises from the *residence chain*
- *Criminal record* used in other chains within the EU, in the *employment chain*, for example.

We have not yet gained much experience of chain-computerisation systems of that nature. At least, there are no examples of success at this level that I am aware of. Nevertheless, according to the insights of *Chain-computerisation in the constitutional state*, selective communication systems concerning criminal records do indeed have a good chance of success and can prevent many flawed

decisions in chains, which cannot be said for a centralised European criminal registry.

Let us take a closer look at hurdle 1. That hurdle can only be taken cleanly if a foreign criminal conviction is 'booked' for the right person. That is only possible if a thorough biometric verification is performed with forensic precision from the country of residence at the beginning of the criminal case elsewhere in the EU. Even in the country of residence itself that often turns out to go wrong. The record in our country is someone with more than a hundred aliases! We cannot establish from the administrative records which of those aliases is his true identity. And neither can the administrative records tell us unequivocally whether the other aliases are real identities of accomplices or of innocent victims or are fictitious ones that have found their way into the judicial documentation.

figure 4

Transfer of sentencing information in the EU criminal law chain

the **'chain level'**

NL-Fingerprint verification (HAVANK)

person known→ fingerprints correct

chain information system

right person → right record

Spanish sentence for NL- resident

transfer

source registers

NL-criminal record

Key: ⟷   interface between sources registers

⟷   interface between source register and chain information system
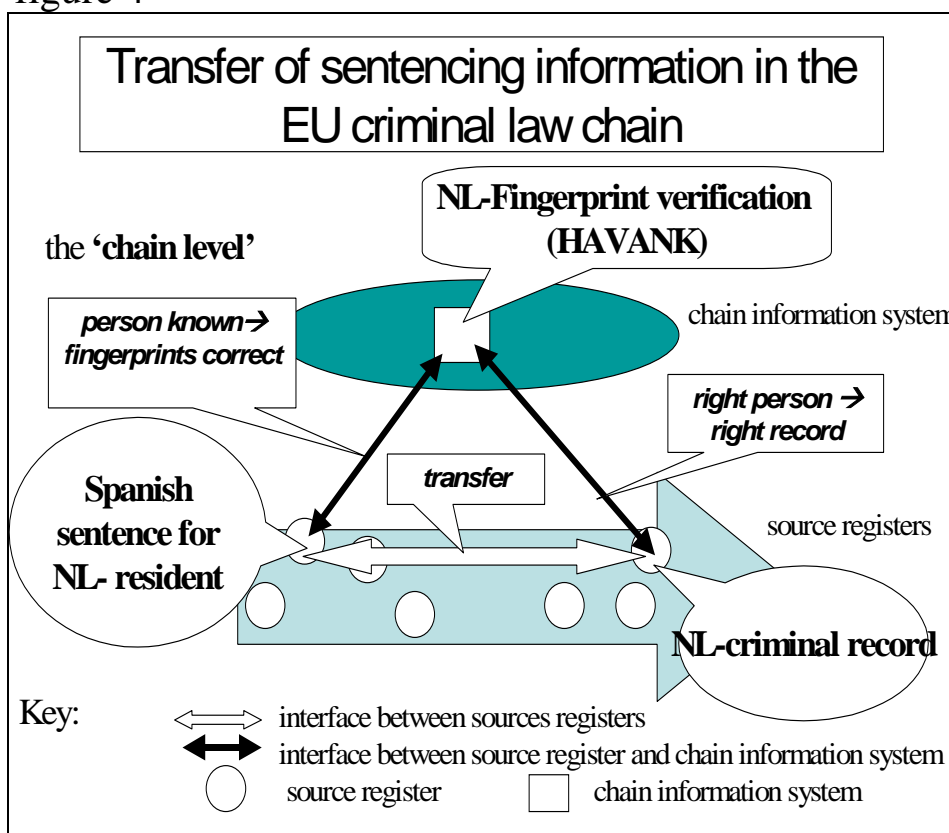
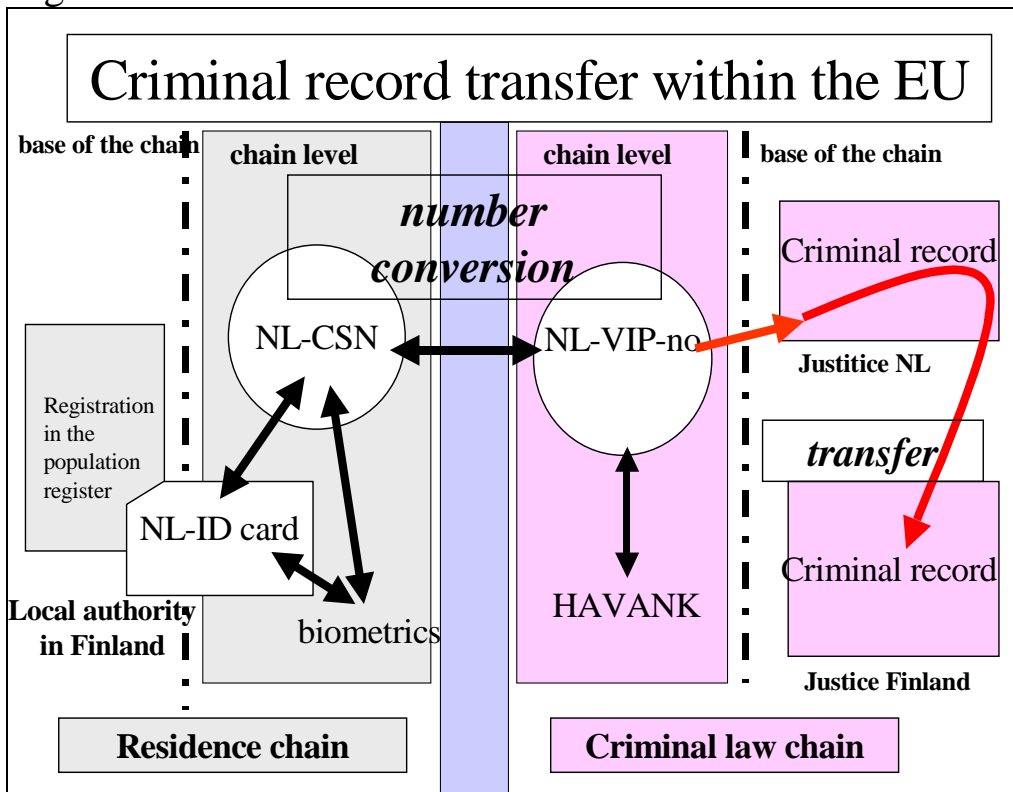◯   source register   ☐   chain information system

Figure 4 shows how a Spanish conviction for a resident of the Netherlands can end up in the right criminal registry. For forensic fingerprint verification, the Netherlands uses the HAVANK system, which provides for each set of fingerprints a list of all aliases that a person has used in Dutch criminal cases. This biometric verification at the chain level directs the Spanish sentence details to the criminal record of the right person. This record is kept at the base level in the chain in the Dutch criminal registry. An EU-wide information infrastructure featuring remote forensic fingerprint verification *from the country of residence* is an absolute necessity. Otherwise, the more cunning villains will seize the opportunity to use aliases from a different EU country which cannot easily be refuted outside the country of residence, in order to keep their own criminal record clean or as short as possible.

Hurdle 2 is the transfer of someone's criminal record as a whole in the event of an international relocation within the EU. After all, the criminal record and relocation within the EU form part of two different chains: the criminal record part of the *criminal law chain* and the international relocation part of the *residence chain*. The transfer of the criminal record itself remains within the criminal law chain, but must now be automatically elicited from the residence chain. That steering process must be embedded in a local work process within the residence chain such as 'registration' at a local authority. Figure 5 describes the communication for a Dutch resident wishing to settle in Finland. It will soon be possible to verify the holder of an identity card bearing his citizen service number using his corresponding biometric details. After a number conversion, if possible also using forensic biometric verification in HAVANK, there is sufficient certainty about proper correlation between the person concerned and his criminal record, if any, to transfer it to the Finnish Ministry of Justice. These transfers should take place automatically, without human intervention, in order to avoid errors and delays. According to the insights of *Chain-computerisation*, they will otherwise be difficult to avoid in the

communication between two chains with different dominant chain problems. First, the residence chain has little self-interest in the accurate transfer of a criminal record in the criminal law chain. And second, the Finnish civil affairs officer has nothing to do with somebody's criminal record at the point of registration if there is no new suspicion of a Finnish crime. Therefore, according to our legal standards this communication system must keep the processing of information in the criminal law chain separated from that in the residence chain. I shall return to this point when I say something more about what is meant by *'in the constitutional state'*.

figure 5

Criminal record transfer within the EU

base of the chain — chain level — chain level — base of the chain

number conversion

NL-CSN — NL-VIP-no

Criminal record
Justitice NL

transfer

Registration in the population register

NL-ID card

Local authority in Finland

biometrics

HAVANK

Criminal record
Justice Finland

Residence chain

Criminal law chain

At EU scale the outlined communication system underlying the transfer of a criminal record to a new country of residence is in itself an unprecedented challenge, but that is not yet enough to solve our communication problem. That is because the criminal record located in the criminal law chain now has to be actually used for decisions in *all sorts of other chains* in all EU countries, such as in

the 'employment chain' for the appointment of a school caretaker. Hurdle 3, then, calls for communication between the criminal law chain and an *alternating* second chain. That is shown in figure 6. The new Finnish resident and his former Dutch criminal record are screened via his Finnish social insurance number for risks related to his appointment. The first step is automatic verification of whether this person has been assigned a Finnish criminal law chain number. If so, after the number conversion a check is made to establish whether there are impediments to the appointment in his (now Finnish) criminal record. It is only if there is a 'hit' that the Finnish decision-maker is notified *that* there are impediments, but not *what they are*. In this communication system, number conversion again makes it possible to keep the information housekeeping of the employment chain separate from that of the criminal law chain.

figure 6

Use of transferred criminal record for appointment of the new Finnish resident to a sensitive job position
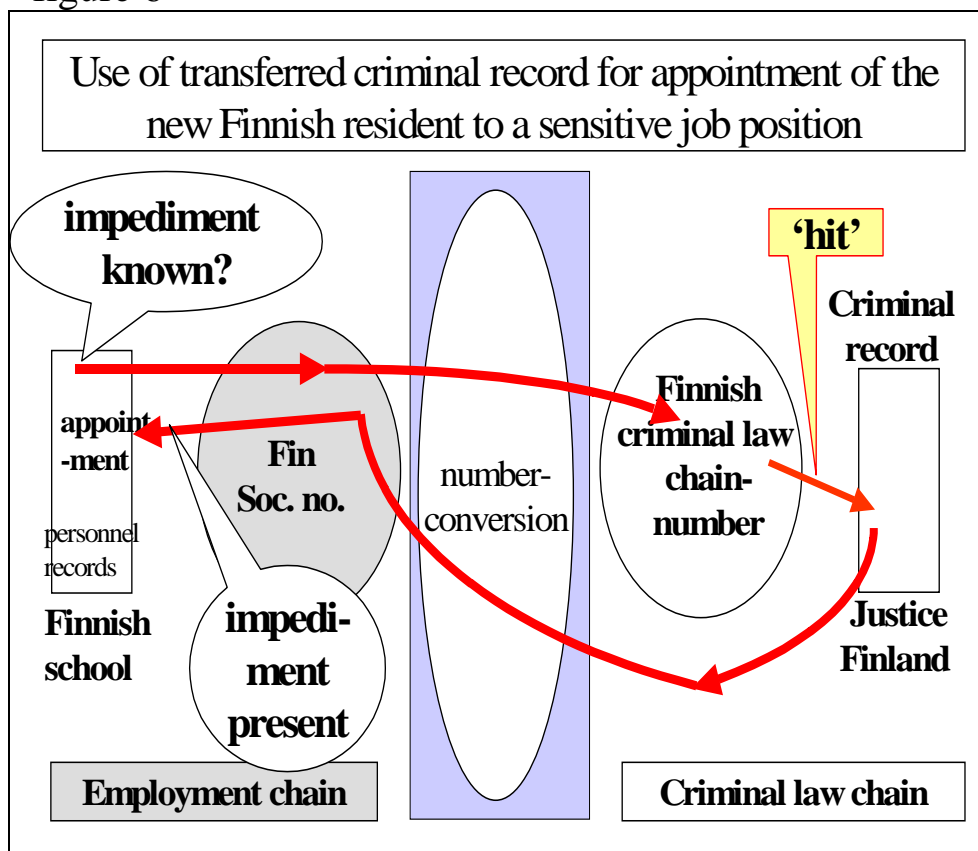
This example clarifies the complexity of our society when viewed from the perspective of large-scale information exchange. It is not my intention to scare you off with this rough chain analysis. I just thought it would be better to do a chain analysis together rather than simply talk about it. Although the concept 'chain' is of course no more than a mental construct, I hope that I have adequately shown that it can be used to show the way in the complex chain landscape of our emerging information society. Unfortunately, a more simplistic approach does not alter the complex reality. Moreover, if seen from a chain perspective, the computerisation of society turns into something fascinating and exciting. I have comprehensively explained the example of the EU criminal registry because the model can stand for communication complexes related to identity records and patient records. These huge communication systems form cornerstones of our future information society. The discipline *Chain-computerisation in the constitutional state* provides tools that can be used to design and create these communication systems. If my field of study can help with the development of these three social priorities (criminal record, identity record and patient record) in the years to come, I will be able to look back with satisfaction on my combined The Hague-Utrecht period.
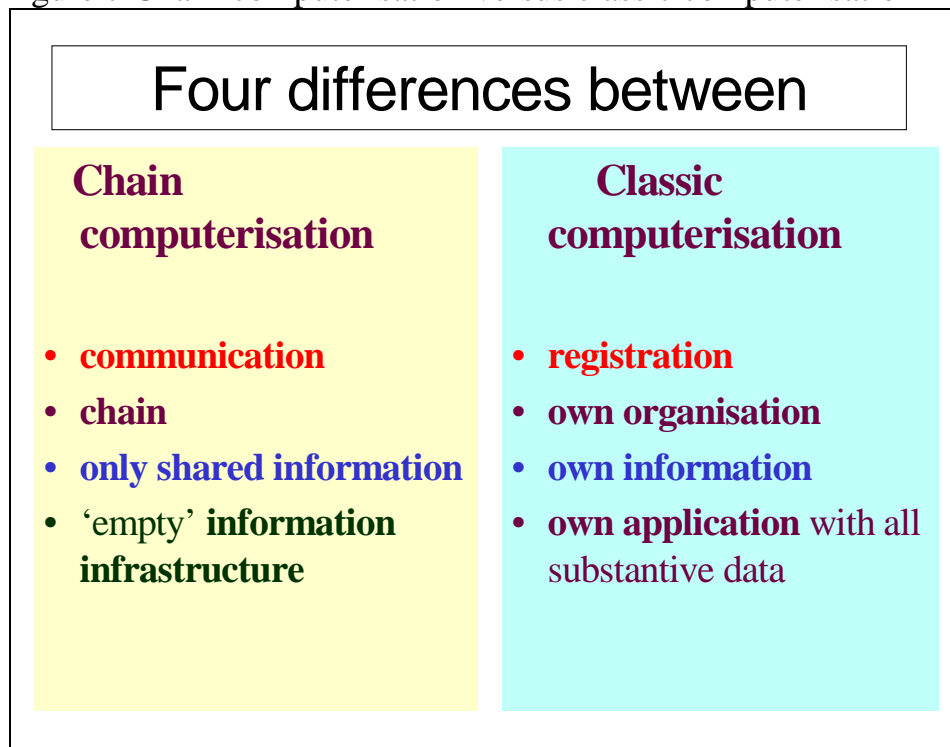
There are still too many people who believe it is necessary to stuff all of the information in a chain into a single database. At this enormous scale, that yields little more than a concentration of management activities, not communication. And that management must be carried out by people who have barely any affinity with the registered details. It would be much better if all parties in a chain collected and managed their own information. A single, collective registry will not work at this scale. Information must stay with the owner and be managed there too. At the same time, chains need a central access system, including a method for signals and alerts, so that other parties in the chain can gain access to the essential information when necessary. What is remarkable here is

that the access mechanism differs between chains. For someone who has had a heart attack, it is important that a small number of details are immediately available to the treating doctor so that he can effectively intervene. The chain will therefore have to be able to supply those details as quickly as possible. That communication system is completely different from that for diabetics, for instance. For the correct treatment of a wide range of ailments for the rest of a diabetic's life, many different care providers require highly varied details.

Chain-computerisation, then, relates above all to structuring and automating the communication needed for the mutual exchange of the information required by all participants in the chain. In that respect, chain-computerisation is essentially different from the usual approach of computerisation. Figure 7 shows the four most important differences.

figure 7 Chain-computerisation versus classic computerisation

Four differences between

Chain computerisation	**Classic computerisation**
• **communication**	• **registration**
• **chain**	• **own organisation**
• **only shared information**	• **own information**
• 'empty' **information infrastructure**	• **own application** with all substantive data

First of all, chain-computerisation focuses on the *communication* of just a few details that are critical to the chain, rather than on the *registration* of these and other details. The key question here is where the necessary piece of information can be obtained at the right moment from elsewhere in the chain in order to avoid a wrong decision at the right place. The question of how that piece of information must be registered and managed somewhere in the chain does not play any particular role in that respect.

Secondly, in chain-computerisation everything revolves around the *chain*, rather than the *individual organisation*. The analysis of information problems and the development of information systems are traditionally based on the client's internal organisation. Conversely, chain-computerisation opts for the external collective 'chain level' as the starting point and focuses on the dominant chain problem. Other than that, 'chain-computerisation' assumes that each chain partner takes his own computerisation process seriously. 'Chain-computerisation' does not therefore compete with the customary, organisation-based approach of automation by the chain partners, but supplements it with a chain-specific communication system that brings about communication between the parties when necessary, rather like a traffic regulator.

The third point of difference concerns the data. 'Chain-computerisation' focuses exclusively on the essential *collective data*, and even then only to the extent that they are indispensable to tackling the relevant dominant chain problem. Conversely, organisations are primarily accustomed to bringing together and managing *all of the substantive data* that they need in their work.

Finally, the fourth point of difference. A critical piece of information can only be made directly available at the moment of a decision or action by means of a chain-specific, 'empty' *information infrastructure* that is geared to the dominant chain problem to be collectively tackled. 'Empty' means that only essential data with-

out much content are present at the chain level. With a reliable patient number at chain level, for instance, it is possible to establish whether each new prescription shows any contra-indications in the light of all current prescriptions for that patient, even though the details of his medicines are held in dozens of different *internal information systems* owned by pharmacists and physicians.

Chain-computerisation in the constitutional state

I now come to the meaning of '*in the constitutional state*' in the title of the chair. It is intended to indicate that fundamental legal principles must serve as the starting point or, in other words, as the design criterion for information infrastructures for large-scale chain communication.

This can be clarified by way of example[3]. Megan's law, or a variant of that law, has been adopted in more than forty US states for the protection of children. According to this law, the entire residential district is informed if a convicted paedophile moves to the neighbourhood. The law was named after a seven-year-old girl who was raped and murdered in 1994. The perpetrator – with two previous convictions for paedophilia – lived in the house opposite the victim's. This American law apparently interprets the idea of 'communication' as 'broadcast'. In our legal culture, we generally take the view that this form of exchanging sensitive personal information is not legitimate. Chain-computerisation in the constitutional state views communication as 'signalling' or 'alerting' somebody if he has to make a concrete decision that could turn out badly without that critical information. The metaphor of private 'mail' is more appropriate than that of public 'broadcast' to this signalling process. A neighbour with children does indeed need to be alerted, but the dissemination principle of public broadcast of Megan's Law is rarely the right - and certainly not the only - response to a pressing social need for better communication.

---

[3]   NRC Handelsblad, 3 December 1998, Profile, p. 2

In the practical case of the EU criminal record we saw twice that in the communication from the one chain to the other, the one chain number was converted into the personal number of the other chain. Personal details from the criminal law chain, for instance, are thus hidden from authorities in the residence or employment chain. The number conversion ensures that personal details from the one chain cannot simply be linked to details from another chain. Chain-computerisation in the constitutional state, then, opts for the protection of people's private lives as a starting point for communication solutions by applying at chain level the principle that data may only be used for the purpose for which it was collected. While someone's criminal record is accurately transferred to the new country of residence, number conversion prevents it from being visible in the residence chain that somebody has a criminal law chain number or a criminal record. And in the criminal law chain, the person concerned is left alone for as long as there is no concrete suspicion of a new criminal offence. Whether this solution will actually work does of course depend on all sorts of other factors, such as the chance of identity fraud being committed in the international relocation. After all, a citizen with a criminal record is not necessarily going to be a cooperative citizen. He may try to rid himself of his criminal record. If he systematically succeeds in that, part of the serious crime problem will shift to the neighbouring country offering the best chance of successful identity fraud. With the EU criminal record based on the country of residence principle we then jump from the frying pan into the fire.
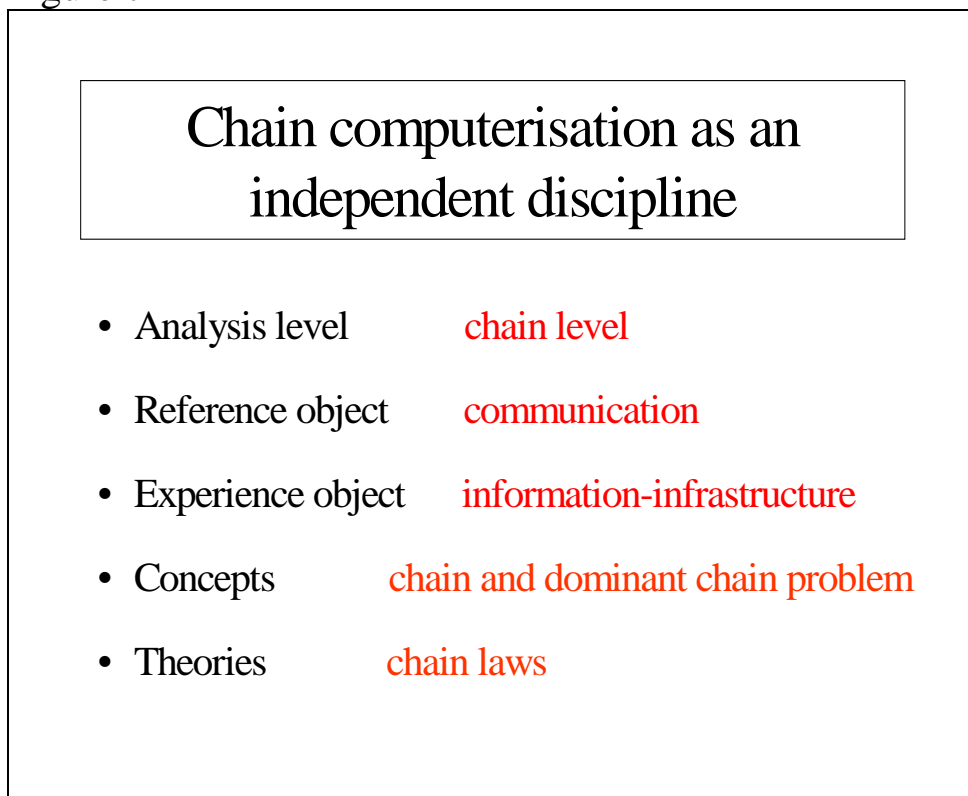
'*In the constitutional state*' also has a second meaning. Social chains are gaining more and more international offshoots and interpenetrations. If the law serves as the starting point for chain information infrastructures, it will become increasingly often the case that several legal cultures, which are sometimes difficult to reconcile, are found within the same chain. This is something that must be taken into account with chain-computerisation. In practice, we are confronted by this in the demands of the US regarding trav-

ellers' details. What is required here is greater understanding of the ways in which various legal-cultural starting points can be given a place alongside each other in computerised chain communication. As things stand, we often choose the solution of the party that has the greatest say in the matter. But insofar as these legal-cultural differences relate to EU countries mutually, that is not a future-proof strategy. After all, within the EU we generally base our approach on the principle of reciprocity.

Chain-computerisation as an independent discipline
I am pleased to have the opportunity today to say something about the position of *Chain-computerisation in the constitutional state* within the broad framework of information and computer sciences.

figure 7

Chain computerisation as an independent discipline

- Analysis level   chain level

- Reference object   communication

- Experience object   information-infrastructure

- Concepts   chain and dominant chain problem

- Theories   chain laws

Chain-computerisation in the constitutional state can be regarded as a sub-discipline in itself because it features all[4] of the characteristics required for that purpose. Figure 7 provides a summary of these criteria. Other information and computer sciences substantiate the five criteria differently. Staff and students can take this as a basis for identifying synergy options for multidisciplinary cooperation or for integration of subject matter.

Education and research
This brings me to my final point: education and research. I have been pleasantly surprised by my first teaching experiences. More insight into the complex interweaving of chains in an emerging information society proves to be inspiring to students. They understand that it is their generation that is facing the challenge of building a liveable information society. My field of study enables them to develop their own tools and knowledge. *Chain-computerisation in the constitutional state* contains essential know-how for students of information and computer science and public law. It should in the future be the case that a professional definition study for an information system is not produced without a sound chain analysis. That will promote the awareness that internal information issues are often related in some way to external chain problems and cannot be tackled exclusively with an internal information system. The benefit of this to students of public law, for example, is that they gain clearer insight into the feasibility of rules and the role played by legal principles in the exchange of information for the implementation of government policy.

The social interest of chains calls for a long-term programme of scientific research into chain cooperation and the information infrastructures required for that purpose. The theory that is now available must be further detailed and supplemented. Existing information infrastructures must be described and analysed by func-

---

[4]   This follows the approach that Lionel Robbins applied to the scientific positioning of the economy in *An essay on the nature & significance of economic science*, MacMillan & Co, London, 1932

tion, history and effects. For students, there are many interesting subjects here for socially interesting graduation research. Such subjects could include the information infrastructures for work and income, the treatment of drug addicts, financial services, automobility, criminal law enforcement and immigration. In addition, the concept of *Chain-computerisation in the constitutional state* will have to be made more broadly accessible. I would like to be able to conclude my professorship in a number of years with the publication of a handbook in the English language.

Word of thanks

Ladies and gentlemen, now that I have reached the end of my lecture I would like first to express my gratitude to the Ministry of Justice for granting me leave to work for one day a week at the University of Utrecht on extending and disseminating the concept of chain-computerisation in the constitutional state. It is a challenge to apply the fundamental principles of the modern constitutional state to computerised external communication.

I would like to thank the members of the University Board, the Rector, the Deans and staff of the faculties of Mathematics and Computer Science and Law for recognising the value of *Chain-computerisation in the constitutional state* and for placing their confidence in me to give this new discipline an identity of its own. I am greatly encouraged in that respect by the remarks of the Chairman of the University Board at the opening of this academic year on the importance to the University of Utrecht of cooperation between disciplines and of internationalisation. Chain thinking leads to greater understanding of the international offshoots of social chains and to cooperation between information science and public law with a view to legal-cultural differences in the international exchange of information. Chain-computerisation in the constitutional state can thus make a contribution to the Board's policy of making studying in Utrecht a more attractive proposition to foreign students.

I am obliged to my colleagues in and around the Ministry of Justice for the countless inspiring and critical discussions about chain issues over so many years. I hope that they will continue long into the future.

I would also like to thank my colleagues in both faculties for which my chair is intended for the pleasant way in which they have welcomed me into their midst.

And finally, a special word of thanks to my wife and sons for their support in bringing my ideals to fruition and to my friends and acquaintances, many of whom are present here today, for their enthusiastic interest in my life and work.

Suggestions for further reading:

1. *Chain-computerisation for interorganisational policy implementation*, in: Information Infrastructures & Policy 6 (1997-1999), IOS Press, Amsterdam, maart 2000
2. *Chain-computerisation for better privacy protection*, in: Information Infrastructures & Policy 6 (1997-1999), IOS Press, Amsterdam, maart 2000
3. Biometrics and Privacy, in: Computer Law and Security Report, May/June 2001, vol. 17 (3) 2001, pp. 154-160, Elsevier Science Ltd, Oxford, UK , ISSN 02673649
4. *Personal numbers and identity fraud, number strategies for security and privacy in an information society,* Part I en II, in: Computer Law and Security Report, vol. 18 (5 en 6) 2002, pp. 327-332 en pp. 387-395, Elsevier Science Ltd, Oxford, UK , ISSN 02673649
5. *Identity fraud as a challenge to the constitutional state*, in: Computer Law and Security Report, vol. 20 (1) 2004, pp. 29-36, Elsevier Science Ltd, Oxford, UK , ISSN 0267-3649
6. *Two barriers to realizing the benefits of biometrics*: A chain perspective on biometrics, and identity fraud as biometrics' real challenge, in Optical Security and Counterfeit Deterrence Techniques V, edited by Rudolf L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE Vol. 5310, pp. 90-102 (2004). Also in: Computer Law and Security Report, vol. 21 (2), March-April 2005, Elsevier Science Ltd, Oxford, UK, ISSN 0267-3649