ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Professional article

Privacy by design on the crossroads of chains

Lessons from the chain of criminal justice in the Netherlands

W.L. Borst

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2013 – Volume 4, Art. #5

Received: 11 March 2013
Accepted: 7 June 2013
Published: 19 June 2013

2013 – Volume 4, Art. #5
URN:NBN:NL:UI:10-1-114603
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Publisher: Igitur publishing, in co-operation with the Department of Information and Computing Sciences, Utrecht University

Privacy by design on the crossroads of chains

Lessons from the chain of criminal justice in the Netherlands

W.L. (Wim) Borst
Ministry of Security and Justice
Post-box 20301, 2500 EH Den Haag, the Netherlands
E-mail: w.l.borst@minjus.nl

Abstract: When officials or organizations in the public domain exchange information on individuals, the privacy and the protection of personal data is at stake. Nevertheless, they have to exchange information and data on individuals in order to "do the right things" regarding these persons; for example suspects or convicts, children in child protection-cases, aliens, patients in public health care situations. The danger of violation of these rights is even greater when information is exchanged between officials from various disciplines or chains. And likewise when the exchange is not incidental (related to one specific case), but structural and automated, i.e. not between officials but between computer systems (databases). Safeguards have to be taken to minimize the violation of the rights of privacy and data protection. In this article it is argued that privacy by design can help control the risks, both within chains and when chains intersect. At first sight, from an efficiency viewpoint and the "need to share" it might seem attractive to match the identifying personal data on subjects as widely as possible (for example store them in one database, which is accessible for all officials or organizations involved). This results, however, in too broad a collection of data, beyond the "need to know", and, therefore, is unnecessary and illegitimate. Identifying personal data should in principle not be matched structurally across chains, but only when necessary in a specific case or when explicitly allowed or prescribed or implicitly required by law.

Keywords: criminal justice chain, chain-computerisation, exchange of information, privacy, privacy by design, intersecting chains, multi-disciplinary cooperation

1 Chains in the Public Domain

Products do not emerge out of the blue; they result from human effort. This effort consists of a number of activities. A sequence of activities builds a process. Products, therefore, are made in processes. This applies to goods as well as to services, both in the private and the public domains. When a process comprises a logically-necessary sequence of activities we speak of a chain. In the classical definition of Thompson: "(*A) must act properly before (B) can act; and unless (B) acts, (A) cannot solve its output problem*" (Thompson, 1967, p. 54). Whereas Thompson had organizations in view, nowadays the concept of a chain is oftenest applied to sequentially defined processes running through a number of organizations (as actors in the process), which are all administratively speaking more or less autonomous, i.e. relatively independent of each other (Kumar & Christiaanse, 1999; Christiaanse, Kumar & Lam, 1999). This provides us with the challenge of chain coordination: a high degree of interdependence at operational level, combined with a high degree of autonomy at administrative level.
Take, for example, the case of a person caught in a traffic incident in which one of his legs is broken. An ambulance is called in and he is carried off to hospital. There

he is operated upon and cared for during the next few days. Soon physical rehabilitation starts, after which he faces the challenge of reintegration into social and professional contexts. These activities taken together show a logical sequence, which runs in one direction: reintegration follows physical rehabilitation; rehabilitation, however, is pointless unless the patient has received treatment and the broken leg has been operated upon; and the operation in its turn cannot be carried out if the patient has not been taken to hospital. At the same time the different organizations that are involved in the process, enjoy a high degree of autonomy and act administratively independently.
The same holds for the chain of criminal justice. The basic process is very simple (cf. Borst, 2011):

investigate → prosecute → try → execute (the sentence) → reintegrate

The police or other investigative authorities investigate the case. If they can gather enough evidence against the perpetrator, they hand the case over to the public prosecutor, or, in the case of some minor offences (at any rate: in The Netherlands) immediately to the Central Fine Collection Agency (Centraal Justitieel Incasso-bureau, CJIB). The public prosecutor assesses the case and either imposes a fine himself (and as a consequence informs the CJIB of the decision so that the agency can execute the sanction) or takes it to court. The court tries the case and imposes a sentence, which is being executed either by the CJIB (financial sentences) or by the Agency of Correctional Institutions (Dienst Justitiële Inrichtingen, DJI: imprisonment), or, in case of community service, the probation service (Reclassering).
So in a chain we see a logically-necessary sequence of activities, which runs into one direction. Each previous step is a necessary condition for each subsequent step. Necessary, but not per se sufficient. In practice the flow may be hampered by a variety of causes. The victim in the traffic accident may die, because of unexpected complications during the operation. Or reintegration may fail as physical rehabilitation fails. In the criminal justice process not enough evidence may be found, or the accused may accept an offer made by the police to pay a limited fine, so that neither prosecution nor trial follows ("attrition"; see for example The Swedish National Audit Office, 1999, p. 14; 2000, p. 14), or, if taken to court, the accused may be acquitted for lack of evidence.
Shortly, the criminal justice system is an excellent example of a chain. Reintegration follows detention (in practice the reintegration process commences while the prisoner is still detained); detention (at any rate: under the rule of law) can only be executed on the basis of a judicial decision; but a judge cannot make a decision unless the case is presented to him by a public prosecutor; and a public prosecutor (again: under the rule of law) cannot take a criminal case to court, if he has not received sufficient evidence from the investigative authorities (such as the police).
The chain of criminal justice, however, is not the only chain in the public domain; not even in the domain of Security and Justice. Within the domain of Security and Justice, for example, we find two more chains of major importance: the "aliens chain" as it is being called in The Netherlands (i.e.: entry, admission, supervision and stay of aliens) and child protection. Not seldom is a person subject to interventions within more than one of these chains, for example a juvenile offender, a juvenile alien or an alien committing crimes. Besides, over the last decades criminal policy has placed increased emphasis on prevention of recidivism by and reintegration of offenders. This policy has resulted into a greater structured effort, in which various organizations within and outside the criminal justice domain, such as those involved with health care, income and work, education, housing and welfare, collaborate in their involvement with a person. This is called the "person-

centred approach". Municipalities are increasingly being made responsible for coordinating these multi-organizational efforts. All these activities are the elements that, linked together, comprise a chain and, at least as regards the public domain, are regulated as such in legislation. And all these activities require cooperation between officials or agencies within chains and even between chains. Cooperation requires the exchange of information. It is right at this point that the struggle begins between the "need to share" (the necessity to exchange information effectively and efficiently) and the "need to know" (the legal and legitimate requirements of privacy and data protection). In the rest of this article I will sketch how within the Netherlands the struggle of the exchange of information when chains intersect, is being dealt with.

2 The Chain of Criminal Justice

My starting point is the chain of criminal justice as laid out before. In this chain numerous officials within hundreds of (semi-)autonomous organizations are working on hundreds of thousands of cases. A number of these cases, however, relate to one and the same subject as a suspect or a convict. Given the desirability or even necessity of a person-centered approach, the officials or agencies concerned have to cooperate – and therefore to exchange information. Each of these officials and organizations gathers information. A basic question for each one of them is: what do we already know about this person; for indeed much information is already available within the chain about many of the suspects and convicts. Yet not always within the official's own organization or domain. For example, when a suspect is arrested and brought in at police station at night, the police officer has to decide whether he will release this suspect after interrogation, or lock him in. To this end the officer wants to know – amongst other things – whether this person is a first offender or a recidivist. In The Netherlands this information is not stored within the police organization or even within the domain of the police; it is stored in a national database outside the police domain. Nevertheless, the police officer is in need of a quick and reliable answer to the question afore-mentioned. Likewise he should know whether there are other current cases pending in relation to this suspect, perhaps in other agencies or in other regions of the country. Again, this information is not available within the organization or even the domain of the police itself, but stored in a national database outside the police domain.

However, there is another question, which is of paramount importance. That question is: who in fact is he or she, now standing before me, concerning whom I have to make a decision? Having information about a person is one thing; but the information is useless, and perhaps even dangerous, if it does not regard the right person. The assessment of the identity of a suspect or convict is a kind of preliminary question in each case and in each decision to be taken in criminal matters. It goes without saying that it is of paramount importance that the identity of suspects and convicts is ascertained in a univocal manner throughout the entire chain. Agencies exchanging information are to trust that the information they exchange, really regards one and the same person. Otherwise the exchange of information would be useless, without effect, a waste of collective means, illegitimate and perhaps even illegal – and so will be the subsequent decisions and actions, based on that information. They have to ascertain that the information gathered really regards the person concerned – and, therefore, that the identity of the suspect or convict is assessed as thoroughly, reliably and unequivocally as possible – before taking any action or exchanging any information. There should be no uncertainty as to the identity of the person about whom information is exchanged, neither should there be any discussion about the way of depicting him

(his name, address, birth and/or place of birth, identification number, etc.). How should this be realized?
In the Dutch criminal justice system the following approach has been chosen. All the data needed to identify a suspect or convict are in principle gathered by the police (or other criminal investigation authorities) at the outset of a criminal case. It is sent to a central database, held by the minister of Security and Justice, the Criminal Justice Chain Database (Strafrechtsketendatabank, SKDB). In this database the identifying administrative data of all suspects and convicts are stored, together with (if available) the copy of the suspect's identity document and his photo. In another database, also held by the minister of Security and Justice, the fingerprints (when available) are stored. These three items: identity document, photo and fingerprint, taken together unequivocally define a suspect's identity. They are stored and managed centrally and once-only. A unique number is assigned to the suspect, which defines his relation to the criminal justice system: the Criminal Justice Chain Number (Strafrechtsketennummer, SKN), and all the information concerning him is linked to that particular number. The identifying data in the Criminal Justice Chain Database (SKDB) is to be used by all officials and agencies throughout the chain, in the various stages of processing the case; and all officials and agencies within the chain on exchanging information on suspects and convicts are required to use the Criminal Justice Chain Number (SKN) as a unique and identifying key. This system and approach was developed gradually during a period of almost two decades (starting from 1993) and enacted ultimately in 2010.
The Criminal Justice Chain Number (SKN) evidently serves the effectiveness and efficiency of the criminal justice system. However, it also serves the privacy of the person concerned. After all, it screens off the domain (or chain) of criminal justice from all other domains. And separation of domains serves as a privacy enhancing provision (cf. Grijpink, 2000).
So far, so good for the chain of criminal justice. But what when chains intersect?

3 On the Crossroads of Chains

As indicated earlier in this article, chains do not rarely deal with one and the same person (client) and, as a consequence, need to exchange information. Here the conflict between the requirements of the primary process and those of privacy and data protection comes in. For data cannot and should not be exchanged limitlessly and freely among public officials and/or agencies; and at any rate not automatically. The Council of Europe's 1981 "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", for example, stipulates in article 6 that "*(p)ersonal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions*." Likewise, the 1995 EU Data Protection Directive (95/46/EC) in article 8 states that "*(m)ember states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*". To these "*special categories of personal data*" article 9 of the 2012 Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) adds "*genetic data*" as well as "*criminal convictions or related security measures*". (To this an EU 2012 Proposal for a Directive of the European Parliament and of the Council adds special rules on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data;

or in short: for the exchange of information in the domain of criminal justice.) So when for example officials from the chain of criminal justice consult with their colleagues from the domains of health care, juvenile protection, housing, education, welfare, work and income, as frequently happens, in particular in the cases of recidivists, each one of them is bound by rules and principles for the exchange of information regarding his own domain. This severely restricts and reduces the amount of information to be shared. Even more so when such information is to be processed automatically – which nevertheless is the desire of many of the agencies and officials concerned. In The Netherlands, at the moment, we see many larger or smaller information systems being created with the aim of supporting the multi-agency collaboration described at the start of this article, for example in the form of "case consultation". Agencies have a need and tendency to bring together information regarding recidivists, juvenile offenders and other categories of offenders. Of course such consultation is of paramount importance to effective conduct on the part of the agencies in relation to dealing with crime and delinquency. But they all wrestle with how to balance the requirements of the primary working processes with the requirements of privacy law and regulation. An intelligent application of the principles of (automated) data exchange is required to help create this necessary balance.

At present, solutions are sought in the concept of "privacy by design". Case consultations for example as such neither have an independent legal existence nor a specific legal basis. Each agency partaking in such forms of collaboration (like case consultation) or in related (common) information systems remains responsible for the information provided to the other parties or stored in a common database. In my opinion these data should not be stored in a common database at all. When in a setting where several organizations temporarily collaborate in relation to a particular individual that requires assistance, care, prosecution, or a combination of these, only the plans of action are to be stored in a common database, but certainly not all the information that individual agencies possess about the individual. The plan of action – the result of the collaborative effort – should be stored for as long as the collaboration and execution of the interventions last. One (and only one) of the parties involved should be responsible for the management of these data. With respect to the data concerning the identity of the person being discussed (the data subject), it should be noted that they *should not* be stored in a common database for the purpose of later use. Whenever information about the data subject is required from other organizations, chains or domains, it should be pulled from existing databases on a national, regional or local level. What is important is that this pulling can be done in a controlled environment, where legal requirements are embedded in the information and technology architecture. For example, when automatically comparing two datasets in various domains using so-called "black box comparison", hits indicate that a subject occurs in the two domains which is the significant and crucial information. This allows agencies to initiate collaboration as it points to the fact that agencies in different domains, independently from each other, concern themselves with one and the same individual. This mechanism is one of many in which the principle of "need to know" is reconciled with the principle of "need to share".

The preceding sketch primarily relates to case-based multi-agency collaboration and for which the parties concerned exchange information. The same principles, however, apply to situations where one organization holds and manages databases for various chains or domains. The mere fact that data are stored under one (physical) roof or even in one (physical) computer (regarded as hardware) does not provide a legitimate ground for combining data being collected by agencies in the various chains. Some organizations are tasked with managing datasets, on behalf of agencies in various domains or chains. These (categories of) data should be stored and managed separately, according to the principles and rules applying to

each of the categories individually. This also applies to the data identifying people. Of course, it can be relevant to know that a person is subject to actions in various chains. And it can be relevant to compare the identifying data from various sources or chains in order to detect identity fraud or identity mistakes for example. However, this does not justify the joining of all these identifying data from a variety of chains into one database and/or matching the data. The matching of data about people is justified only when legislation explicitly prescribes or permits or implicitly requires so. For example: Dutch legislation prescribes that detainees forfeit (unemployment and other) benefits as soon as they are being held captive. This requires implicitly that *every* detainee shall be matched to *all* people receiving benefits (cf. Grijpink, 1999, 138). In such a case an integral match of populations is justified. In all other cases - i.e. when legislation does not justify an integral match of populations - the same procedure can be followed as in the case of case consultation systems described above: a party needing the information can ask or look for it (if he is authorized to do so) or blind "hit-no hit" file comparisons can be executed, if necessary periodically.
Matching data collected for one purpose, e.g. the application of criminal law, to data collected for other purposes, e.g. aliens law or child protection, clearly is a form of "further processing of data". The recent Article 29 Data Protection Working Party "Opinion 03/2013 on purpose limitation", provides an ample discussion of the principles to be taken into account in this field, but, unfortunately, does not in any detail touch on the subject discussed in this paper. It states – as far as relevant for our subject – that the incompatibility of further processing of data should be assessed "on a case-by-case basis", leaving open whether this "case-by-case" assessment applies to individual cases strictly or perhaps also to categories of cases. In the former case, any structural or automated matching of data seems out of the question. That's why I consider the "case-by-case assessment" applicable to categories of cases too. It is exactly this approach which is advocated in this paper.

4 Conclusion: Privacy by Design on the Crossroads of Chains

"*Civilization seems inescapably to bring with it the expansion of interdependencies*", Thompson (1967) sighed nearly half a century ago (p. 156). The course of things ever since has not refuted his sigh. Collaboration of actors and institutions within and across chains increases complexity. This complexity can not be overcome. Architecture, however, is there as a means to cope with it. In this article I sketched privacy by design as a way to master complexity in the exchange of information. The following principles emerge.

- In a chain, centrally, i.e. on chain level, store and manage data on the identity of the persons concerned (the data subjects).
- Furthermore, only centrally and on a chain level store and manage data which are of paramount importance to all parties involved in the chain. In the chain of criminal justice, for instance, this applies to information about (other) current cases and to the suspect's criminal records.
- On the crossroads of chains, only centrally store and manage a minimum of data. With regard to inter-organizational collaboration, like case consultations, only centrally store the data relating to the actions and agreements produced by the collaborative efforts. And store these data only for as long as is required for the collaboration. Make one of the parties involved responsible for the management of the common set of data.
- Even where chains intersect (either in case of multi-chain consultations or in cases where one organization as a kind of service provider manages various databases from various chains) the identifying data of the persons concerned (the data subjects) should be managed chain-wise (for each chain separately).

> The data minimization principle demands that matching of identifying data – if needed – should be done incidentally when possible and integrally only when legislation explicitly prescribes or permits or implicitly requires this.

It should be borne in mind that these principles, as a matter of fact, mainly relate to the automated exchange of information. The afore-mentioned 1981 Council of Europe Data Protection Convention even relates exclusively to "automated processing of data". As it is no use automating tasks or transactions which are performed only incidentally, the Convention therefore mainly applies to forms of structural exchange of information. The 1995 EU Directive and the 2012 EU Proposals (one of which is the intended successor of the 1995 Directive), however, have a somewhat wider scope: they apply to "the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." So when neither data are processed automatically nor being filed in a central database the possibilities of exchanging information increase. In case of immediate danger to the data subject, for instance, in the case of having to "protect his vital interests" much is possible under current privacy law. Just do not carve the data processing in stone by structurally and automatically exchanging information about people. When thinking about the possibilities of and the limits to the exchange of information between public and/or semi-public agencies, the distinction between incidental and structural exchange of information should always be taken into account. This provides an important key to a realm of possibilities to effective inter-organizational collaboration while simultaneously protecting the informational privacy of the subjects concerned.

Biographical notes: Wim Borst (1953) studied Law (1976) at Erasmus University Rotterdam. He got his PhD at Leiden University (1985) with a dissertation on "The means of evidence in criminal cases." In 2006 he obtained the degree of Executive Master in Information Management (EMIM) at Amsterdam University. He taught criminal law at Leiden University and served as a court legal assistant at the Supreme Court of the Netherlands. At the moment, he is senior policy advisor for the Ministry of Security and Justice in the field of information management concerning law enforcement.

References

Article 29 Data Protection Working Party "Opinion 03/2013 on purpose limitation" (00569/13/EN WP 203).

Borst, W.L. (2011). Chain-computerisation in practice: the criminal justice chain. *Journal of Chain-computerisation, 2*, Art. #10.

Christiaanse, E., K. Kumar, H.M. Lam. (1999): Chains, hubs and webs: ICT enabled redesign of inter-organizational forms. *PrimaVera Working Paper 99-22.* (http://primavera.feb.uva.nl/PDFdocs/99-22.pdf)

Council of Europe (1981). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, 1995, No. L 281/31. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML)

Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Brussels, 25.1.2012. COM(2012) 10 final. (http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.-pdf)

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, 25.1.2012. COM(2012) 11 final. (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

Grijpink, J.H.AM. (1999). *Werken met Keteninformatisering* (Chain Computerization in Practice). Den Haag: SDU.

Grijpink, J.H.A.M. (2000). Chain-computerisation for better privacy protection, in: Information Infrastructures & Policy 6 (1997-1999), IOS Press, Amsterdam, 2000, ISSN 1383-7605.

Kumar, K., E. Christiaanse (1999). From static supply chains to dynamic supply webs: Principles for radical re-design in the age of information. *PrimaVera Working Paper 99-14.* (http://primavera.feb.uva.nl/PDFdocs/99-14.pdf)

The Swedish National Audit Office. (1999). *Brotmålskedjan – i Sverige och andra länder. Kartläggning och analys*. Stockholm: Riksrevisionsverket.

The Swedish National Audit Office. (2000). *Performance Audits of the Legal System 1990-1999*. Stockholm: The Swedish National Audit Office.

Thompson, James D. (1967). *Organizations in Action. Social Science Bases of Administrative Theory*. New Brunswick (U.S.A.) and London (U.K.): Transaction Publishers.