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

Scientific article

Chain-computerisation and privacy

M. van der Veen

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

2011 – Volume 2, Art. #11

Received: 1 March 2011
Accepted: 1 April 2011
Published: 14 April 2011
Translation: Sandra R. Reijnhart

2011 – Volume 2, Art. #11
URN:NBN:NL:UI:10-1-101416
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Publisher: Igitur publishing in co-operation with the Department of Information and Computing Sciences

Chain-computerisation and privacy

M. van der Veen
Capgemini Consulting, cluster Security and Justice System Chains
Post-box 2575, 3500 GN Utrecht, the Netherlands
E-mail: maveen@capgemini.com

Abstract: The theory of Chain-computerisation makes a major contribution to *privacy by design* because essential proportionality and purpose limitation of data exchange are central to the methodology. Nonetheless, in spite of the application of the theory, major privacy risks remain. We are going to discuss these risks and offer a solution in the form a privacy scan: the Smart Privacy Approach. This privacy scan is a tool for defining and solving the privacy risks inherent in chain co-operation. This helps in applying the theory more carefully and in taking measures where risks to privacy arise.

Keywords: Chain-computerisation, privacy, 'privacy by design', risk

1 Chain-computerisation and privacy

Privacy protection is a recurring and fundamental issue in debates on the design of the healthcare and security chains. Examples of this are the Electronic Patient Records (EPR), the inclusion of biometric data in passports and the method of dealing with habitual offenders and juvenile criminals. More chain co-operation leads to the growth of a number of systems and interfaces, redundant storage of data and more involved parties which can, in turn, lead to problems in the area of manageability, overview of information flows and (also because of this) privacy protection. The theory of Chain-computerisation was developed in answer to the development of the growing, large-scale chain-computerisation (Grijpink, 1997). One important advantage of this theory is that, from the very beginning, the privacy aspect was included in the structuring of chain co-operation and in the design of chain information systems (*privacy by design*). The theory, moreover, already includes various handles for increasing privacy protection in chains (Grijpink, 1999, p. 137; Grijpink, 2010, p. 16).

However, a supplement to the theory is necessary because, in practice, it works differently than what is, according to the basic principles of the theory, the case. Because of this there are, in spite of the *privacy by design* nature of Chain-computerisation, still major privacy risks which will be described in Paragraph 2. One solution for these privacy problems in a chain is a privacy scan where the risks for the persons involved are central and not a system or theoretical framework. These risks will require reflection on the information process. That could lead to a better application of the theory or to additional mitigation measures.

2 Criticism of privacy safeguards

Chain-computerisation occurs, according to the theory of Chain-computerisation, within a context that is characterised by irrational decision-making, co-operation of parties on a dominant chain problem and data-exchange at a number of levels. The parties in the chain will, in this context, only be able to create minimal, but effective information sharing. The best privacy protection is offered by chain

information systems where no central storage or exchange of source information is possible and databases can only check information through reference indexes. But also in less far-reaching solutions, the chain approach compels a critical attitude towards information-sharing.

It is, however, unlikely that the principles of the theory of Chain-computerisation can be implemented in such a way that they can also actually enforce the intended better privacy protection, because:

- Irrational decision-making can be broken by political pressure, consensus or the provision of more means, such as time, money or subsidies. Difficult questions and problems can be 'bought off;'
- The dominant chain problem will not be sufficiently clearly defined and assessed within an environment that acts less irrationally than the theory presumes. That can lead to the broader use of the minimal dataset and to the exchange of a set of data that is broader that necessary;
- In an environment where co-operation already exists, one is more inclined to choose solutions that can fit easily within the existing structures, which leads to a wider dissemination of data than is necessary (Kouwenhoven, 2007).

Due to these environmental factors, it is improbable that the critical attitude which the application of the theory leads to will be put into practice. More information will be shared and stored than is necessary, with all of the inherent privacy risks. In order to contain these risks, privacy issues will have to be tackled structurally, starting with a better identification of privacy problems.

3 Concretizing privacy: Smart Privacy Approach

In order to better be able to critically assess privacy safeguards in a specific chain co-operation, one must be able to get a better 'grip' on the privacy. First of all, it is necessary to describe and operationalize privacy better. In doing this, we recognise the following problems. First of all, a citizen perceives an invasion of privacy differently than an organisation 'with a mission.' Secondly, the privacy incident frequently takes place on several levels at the same time: from an individual citizen to the level of human rights. Where, for example, is the boundary between a camera as a handy tool and Big Brother? Thirdly, privacy has a huge dynamic from the specific social context such that the boundaries of privacy can change under the influence of incidents. Citizens are inclined to trade privacy for more safety, also because safety is concrete and privacy remains an abstract concept.

In order to make privacy issues concrete, we have developed a structured privacy scan based on the work of Daniel Solove. Solove argues that privacy is an umbrella concept for sixteen information-processing risks between persons and organisation (Solove, 2006; 2008). Privacy is intangible in such a statement as 'interconnectability in chain co-operation violates our privacy'. With the Smart Privacy Approach introduced in this article, the problem could be identified as the 'aggregation of source files increases the risk of erroneous data reuse and the drawing of incorrect conclusions about persons (false positives and negatives) and decreases the verifiability of the data.' After the privacy issues have been made concrete with this scan, specific, concrete solutions can be identified.

The steps in this privacy scan - the Smart Privacy Approach - are:

(1) Description of the privacy issue to be studied. This first step includes the

identification of the chain task and the information processing required for this task. The data flow of personal details forms the basis, such as 'the recording of patient data in a database' is the case with the EPR. Just as in the case of the chain approach, the focus on the issue in question is important and one issue may require several analyses;

(2) The analysis of information risks during the information processing. In this second step, we analyse which of the information risks can occur. It is often the case that only a limited number of the sixteen identified risks play a role here;

(3) In-depth studying of information risks and actors. In this third step, the analysis of the risks for the actors involved is broadened. First of all, it demands that the privacy issue be examined from the broader perspective of a large-scale application. At the individual level, one camera is no problem; for a community, 50 or 1000 cameras could well be. Moreover, it demands that actors are appointed who are, perhaps, not immediately involved in the issue in question, but who are affected by *consequences* of activities. Finally, it demands that the factor of time be included and the risks for actors in the long term are identified;

(4) Identification of the mitigation measures per privacy problem.

4 Results

The result of the Smart Privacy Approach is a structured analysis and clear identification of the privacy issue, an assessment of the risks for the privacy of the parties in question and an insight into the actors involved and the level at which they are acting (local, regional or national). Only then can fitting solutions and concrete actions be identified. The scan prevents important aspects of the privacy issue from being overlooked.

The theory of Chain-computerisation offers the possibility to take an extremely critical look at the necessity and the proportionality of data-sharing and at the direct links between the information processing involved and the purpose limitation for which the information was initially gathered. As an augmentation to chain-computerisation, the proposed privacy scan is a tool for putting the privacy risks inherent in chain cooperation into operation. It thus contributes to a more precise application of the theory and an improvement of privacy within chain co-operation.

Biography: Drs. M. (Martijn) van der Veen (1978) studied Public Administration and Public Policy at the University of Twente and has been studying Dutch Law at the Open University. Since 2006, he has been employed at Capgemini Consulting in the area of organisational change and process improvement, concentrating, since 2008, on the security sector. Privacy, the touchstone of good information governance is one of his areas of special interest.

References

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving* [*Chain-computerisation in practice. An information strategy for an information society*]. The Hague: Sdu Uitgevers.

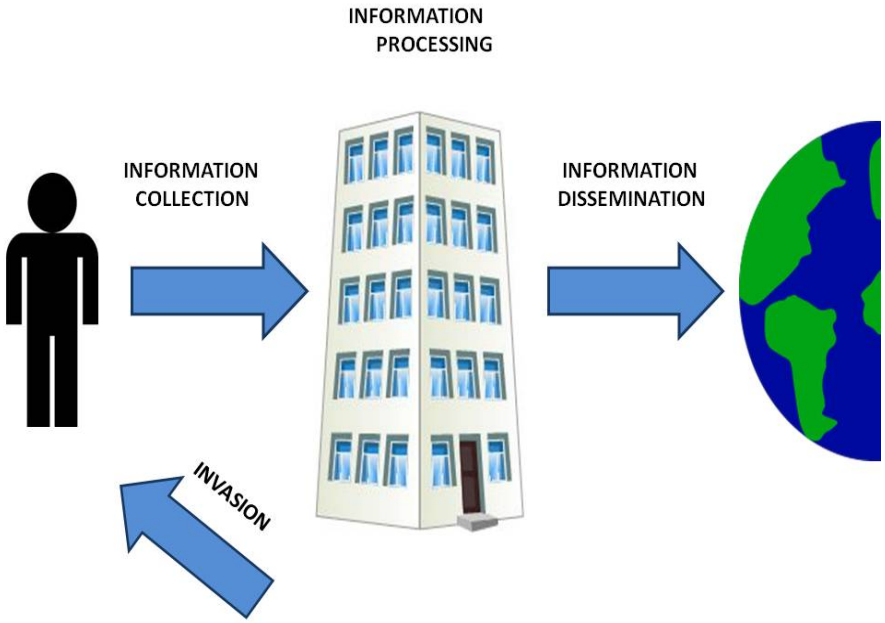
Grijpink, J.H.A.M. (2010). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling* [*Chain-computerisation in brief. Theory and Practice of large-scale information exchange*]. The Hague: Boom/Lemma Uitgevers.

Kouwenhoven, R. & Binnekamp, R. (2007). Ketensamenwerking in de lokale veiligheidspraktijk [Chain co-operation in the local security practice]. In J.H.A.M. Grijpink, T.A.M. Berkelaar, D.G.H. van Breemen, B.P.M.J. Dommisse & R.J. Steenkamp (Eds.), *Geboeid door ketens: Samen werken aan keteninformatisering* [*Fascinated by chains. Building Chain Information Infrastructures together*]. The Hague: Platform Keteninformatisering [Platform Chain-computerisation].

Solove, D.J. (2006). *A Taxonomy of Privacy*. *University of Pennsylvania Law Review, 154*(3), 477.

Solove, D.J. (2008). *Understanding Privacy*. Cambridge MA: Harvard University Press.

A. Appendix: Risks of data processing



Risks of data processing
Information collection
Surveillance
Interrogation
Information Processing
Aggregation
Identification
Insecurity
Secondary Use
Exclusion
Information Dissemination
Breach of Confidentiality
Disclosure
Exposure
Increased Accessibility
Blackmail
Appropriation
Distortion
Invasions
Intrusion
Decisional Interference