Interagency data exchange protocols as computational data protection law.

Willam BUCHANAN[a,] , Lu FAN[a] , Alistair LAWSON[a] , Burkhard SCHAFER [b1] DS
Russel SCOTT[c], Christoph THUEMMLER[a] Omair UTHMANI[a]
[a] *Edinburgh Napier University, Dept of Computing*
[b] *University of Edinburgh, School of Law*
[c] *Scottish Police Colleg. National Intelligence Model Development Team,,*

Abstract. The paper describes a collaborative project between computer scientists, lawyers, police officers, medical professionals and social workers to develop a communication infrastructure that allows information sharing while observing Data Protection law "by design", through a formal representation of legal rules in a firewall type system. .

Keywords. Information sharing syntax; intelligence model; security policy implementation; Role-based security; Police and Public Services; community risks.

Introduction

In 2005, the 17 month old Peter Connolly, known in the press as "Baby P" died from more than 50 injuries that he suffered over an eight-month period on the hands of his mother and her boyfriend. It quickly transpired that he had been seen frequently by Haringey Children's services and NHS health professionals, who had failed however to coordinate their various reports and as a result spot the danger he was in. His was but the last of a number of high profile cases of child neglect and child abuse where victim and perpetrator had been known to several agencies, from social services to hospitals to police, but where due to a lack of data sharing between them, appropriate reaction had not been taken.

At the same time however, the opposite problem also grabbed headlines: Local councils were caught abusing legislation intended to combat terrorism to collect and exchange data of citizens suspected of everything from permitting their dog to foul in parks to lying about their address in applications to schools for their children.

When in the first type of cases, harm ensued because data that should, and legally could have been exchanged between agencies wasn't, in the second type of cases data that should never have been collected in the first place was exchanged without care and precaution between agencies. In theory, a whole raft of legal measures, from the Data Protection Act to the Community Care Act 2003 should have ensured that all and only the necessary and legally permissible data was exchanged. However, regulating data exchange between agencies through legal codes has proven difficult. "Top Level" acts

[1] Corresponding Author.

such as the Data Protection Act use highly abstract language, give only vague guidance on how to balance competing interests, and are too unspecific to be of direct help to personnel that is not legally trained. Inter-agency Information Sharing Agreements that try to operationalise the relevant law have by now become so complex, long and technical in their attempt to cover every possible situation that they are often ignored by practitioners working under sever time constraints. The result is that decisions about data sharing are often done informally, between individuals that trisut each other on a personal level, and with insufficient transparency and audit possibilities. Personal attitudes and professional mentalities, rather then legal rules, decide if agencies "play it safe" by not disclosing important information (fearing actions under the DPA) , or disclosing unnecessarily (in fear of being caught "doing nothing").

Of course, today most of the relevant data is stored electronically, and information exchange requests will also be transmitted using ICTs. This allows us to develop a new approach to data exchange and its regulation, which is at the centre of this paper: Rather then relying on written regulations that are interpreted by people within the different agencies, we show ways in which core concepts of the relevant legislation can be represented computationally, creating something akin to "firewalls" between the agencies that allow transfer of all and only those data that are legally permissible. Our project, a collaborative study involving computer scientists, lawyers and police officers under the aegis of the Scottish Institute for Policing Research, shows how is developing data exchange protocols that represent embed relevant legislation into the software. The user, police officers or social workers, don't have to think any longer (much) about the rules, the system itself ensures they act in a law compliant way.

Larry Lessig [1] popularized the idea that on the internet, regulation through laws is often inefficient, but embedding legal concepts directly into the code, forcing users to behave in a law compliant way, is a feasible alternative. The examples that he uses however, mainly Digital Rights Management systems, are far away from the syntactic structure of legal reasoning and legal concepts. While they prevent illegal copying, and permit legal copying only, they don't represent the concept of property or theft, or at least not any more than a good lock on a door can be said to represent these concepts in the offline world. The AI and Law community historically prefers much more explicit formal representations of key legal concepts, and in particular Sartor and collaborators [2,3] have shown ways in which autonomous agents can be equipped with explicit legal reasoning capacity, including the ability to reason about conflicting values. This ability is particularly relevant in our context, where privacy concerns have to be balanced against the legitimate interested the police ad we hope that ultimately, we will express at least some of the core legislation using this approach. However, for the time being we target a system halfway between Lessig and Sartor: Our approach mimics the outcomes of rather than replicates the legal reasoning process, and a greater emphasis is placed on the bottom up knowledge acquisition process using empirical, socio-legal methods such as large surveys of key personnel. The reason for this choice of priorities is largely pragmatic: Even though data exchange takes place within a framework governed through the DPA by abstract concepts similar to those Sartor formalised, "on the ground" these abstract considerations play a much less important role than the "translations" of these legal concepts into specific professional "ways of doing things" where people not schooled in law have developed their own modes of understanding. Ultimately, these have to be consistent with the top level conceptual

framework, but our analysis of the main reasons for inter-agency communication breakdown indicate that greater impact in the short term can be had through implicit representations as part of a firewall type protocol than the more ambitious explicit modeling of the legal reasoning process

1. Inter-agency data exchange

The exchange of information between the police and community partners forms a central aspect of effective community service provision. In the context of policing, a robust and timely communications mechanism is required between police agencies and community partner domains, including: Primary healthcare (such as a Family Physician or a General Practitioner); Secondary healthcare (such as hospitals); Social Services; Education; and Fire and Rescue services.

Such requests typically form the basis for any information-sharing agreement that can exist between the police and their community partners. It defines a role-based architecture, with partner domains, with a syntax for the effective and efficient information sharing, using SPoC (Single Point-of-Contact) agents to control information exchange. The application of policy definitions using rules within these SPoCs is inspired by network firewall rules and thus define information exchange permissions. These rules can be implemented by software filtering agents that act as information gateways between partner domains. Roles are exposed from each domain to give the rights to exchange information as defined within the policy definition. This work involves collaboration with the Scottish Police, as part of the Scottish Institute for Policing Research (SIPR), and aims to improve the safety of individuals by reducing risks to the community using enhanced information-sharing mechanisms. Agencies are actively encouraged by governments [4] to form partnerships and collaborate to ensure provision of effective community services. Working in partnership by sharing information has been particularly successful in public services [5,6]. Often, partnership working is a requirement mandated by legal directives. In the UK, for example, Acts of Parliament such as the Health and Social Care Act 2001, Police Reform Act 2002, Community Care Act 2003 and the Children Act 2004 all necessitate information sharing among partner agencies.

Barriers to forming effective partnerships and information exchange include lack of trust between organisations; lack of understanding of policies and legislation; and disparate communication systems. The issue of trust can arise from traditional rivalries between organisations that view each other as competitors rather than collaborators [7]. In our context, a more pertinent problem are however caused by incongruent professional values and missions of the different stakeholders. A social worker, trying to establish a trust relation with a young person deemed at risk will be hesitant to pass on information about low level drug dealing to the police, if he fears that the information will result in heavy handed police activity that would make is work impossible [8]. However, evidence suggests that increased government encouragement to collaborate [9], in the form of incentives and legal obligations, has helped in alleviating this situation. Initiatives that highlight best practices and procedures, such as the guidance on the Management of Police Information (MoPI) [10] within the Scottish

and other UK police services, also simplify the interpretation of policies and legal requirements. This ease of interpretation of policies, in turn, alleviates the risks agencies face from non-compliance [11] and, thus, further aids collaboration.

2. Data sharing model

In modern democracies, rightly suspicious of the danger that information can also be abused, data sharing has to take place within tightly defined legal parameters, found in legislation such as the Data Protection Act (1998) in the UK. This act, just like the EU directive that it implements, requires an often difficult balancing act between different legal values. The human right to be "left alone" has to be balanced against conflicting such rights, such as the right to live or property. Put simply, it is more acceptable to invade the privacy of a person under reasonable suspicion to plan a terrorist attack than that of a mother suspected, with little evidence, to have lied about her address on the application for a school place. As a first step to model the legally required balancing acts, we developed four categories of data sharing scenarios that can be found in police work. On each level, different arguments count for or against sharing of data, and the legal analysis differs accordingly

- **Level 1. Community**. This level focuses on community actions, typically using Intelligence Lead Policing, where measures are taken to try and prevent future criminal activities. This is typical in community actions, where information is exchanged in order to reduce a longer term threat, which could become more serious.
- **Level 2. Preventative intervention**. This level focuses on prevention of specific, identified criminal activities, with the requirement to share information will often depend on the seriousness of the criminal activity. A typical example is rescuing a kidnap victim.
- **Level 3**. Crime investigation. This level deals with the investigation of a specific crime. Unlike level 3, which is forward looking, level 3 is backwards looking, a singular past event is the focus, the main harm has already occurred.
- **Level 4. After the event**. This level focuses on consuming data on criminal activity, in order that it can be used in the future to reduce the risk to the public. This involves for instance the compilation of statistics by police agencies. It feeds back into level 1., and also informs activities such as resource allocation by the police

The justification to share information at Level 2 and 3 can be achieved through an information sharing agreement, where relevant criminal contexts can be explicitly defined. For example in a missing person context, a social worker may request the current location of the person from the police, and justify it in this context. When audited, the social worker would then have to provide evidence that the context was correct at the time of the query. A rule can thus be written which defines the context, and the requirements for the information sharing, which is then agreed between the police and the community partner. The information sharing agreement at this level can thus define a **criminal context**. At Level 1 and Level 4, it is more difficult to define clearly a criminal context, as there is no actual crime. Thus these two levels are more based on **abstract societal goals**, where the reason for the sharing are based on the

values that society defines, such as in analyzing criminal activity, and in dealing with a social problem. Any information sharing at this level will thus be build around a value-based system, where individual rights are less prominently balanced against each other. important. An information sharing agreement at this level will thus be agreed upon by defining the values related to information sharing. In this paper we focus on Levels 2 and 3, as the criminal context is easier to define in an information sharing agreement.

3. Information Sharing Framework

The syntax proposed in this paper builds upon the principles of best practice within the Scottish Police, such as those highlighted in the guidance on the Management of Police Information (MoPI). This guidance defines principles for police information management, including the processes and procedures under which information may be requested by, and shared with, partner agencies. Thus, MoPI helps to identify organisational policies and legal compliance issues that affect police information sharing.

Once the need to share information with a partner agency is identified and affected procedures and compliance issues defined, the principles highlighted in MoPI can be used to construct an Information-Sharing Agreement (ISA). ISA's define the agreed specific rules, derived from policies, that direct the recording, access, review and dissemination of information between partner agencies. Usually, agencies that have similar functions also have similar ISAs and can be grouped together into domains. From a Scottish policing perspective, common information sharing domains include Police services (POL), Social Services (SOC), Primary healthcare (HCP), Secondary healthcare (HCS), Education (EDU), and Fire and Rescue (FIRE). MoPI also outlines the concept of a Single Point-of-Contact (SPoC), which describes the individuals who are designated as main contacts for the exchange of information between domains. Any exchange of information between the domains, therefore, needs to occur through the designated SPoCs.

3.1. Single Point of Control (SPoCs)

Figure 1 illustrates the Single Point of Contact (SPoC) concept described in the guidance on the Management of Police Information (MoPI), which is implemented as software agents that serve as gateways for information requests. The function of these SPoC agents is inspired by firewalls within a computer network. At a basic level, firewalls use a defined set of rules to either permit or deny net-work traffic. Similarly, SPoC agents validate requests for information exchange based on rules, derived from organisational policies and legislative requirements, as defined in Information-Sharing Agreements (ISA). This means that the agent attempts to match a request for information exchange against the rules defined in the set of rules in the ISA. If the request does not match a rule, the agent will then attempts to match the request against the next rule and so on. Once a match is found, the agent will carry out the action (permit or deny), as defined by that rule, and end the searching (as a firewall would). If no matching rule is found in the set, the agent will deny the request. This is similar to the idea of an implicit deny criterion used by firewalls where no matching rule is found. In the case that a request is denied, the agent will return information indicating

the reason for the denial. The policies defined in the ISA can take the form of restrictions such as limits on the number of search items returned, specified timeframe of validity for an incoming request, and so on.

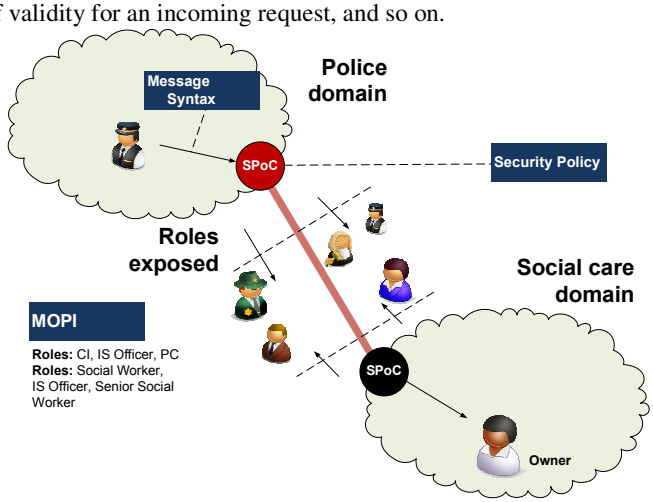

Figure 1: Overview of the architecture

3.2. Role-Based System

A core part of the Information-Sharing Agreement (ISA) is to specify those who will have access to the shared information. Typically, this involves identifying functional roles that need to access information in order to complete a defined task or job. The information exchange syntax thus uses a hierarchy within domains and roles exposed between domains to facilitate the exchange of information. For example, Analyst (ANA) may be an exposed role from the Child Abuse Investigation (CAI) organisational unit in the Police domain (POL). This role is represented as POL.CAI.ANA, illustrating the full hierarchy. Similarly, an Inspector (INS) from the Missing Persons (MPR) business area of the Police domain would then be represented as POL.MPR.INS. For a Social Worker (SW) role exposed from the Children Day Care Service (CDC) of the Social Services (SOC) domain, the representation would be SOC.CDC.SW. Essentially an exposed role is one that has permissions for information exchange from another domain. For example, if Social Workers (SOC.CDC.SW) are allowed to request information from Police (POL), then the SOC.CDC.SW role would be defined in the ISA as having permissions for this action. Thus, the SOC.CDC.SW role is exposed from the Social Services domain to the Police domain.

3.3. Syntax

A syntactic approach to the concept of information-exchange simplifies the creation and implementation of rules. The main reason for this approach is the vast number of disparate information systems that various police divisions and partner agencies use, which can cause difficulties relating to translation and the resulting misunderstandings. The result, often, is that valuable semantics can be lost in the exchange, which degrades the efficiency of the information-sharing mechanism and undermines the objectives for which the information was being shared in the first place. Common logical definitions,

which constrain possible interpretations of any given concept to a finite set, therefore, need to be agreed upon before communication can occur. Figure 2 outlines the syntax of the rule request and of the policy rule, which provide a close match to each other. Most of the fields within these rules are defined within, and generated from, the ISA, but the [Object] field is kept as a free format field, in order that the structure of the databases within the domain does not have to be exposed to other domains. All of the other fields within the rules are thus used to match the request.

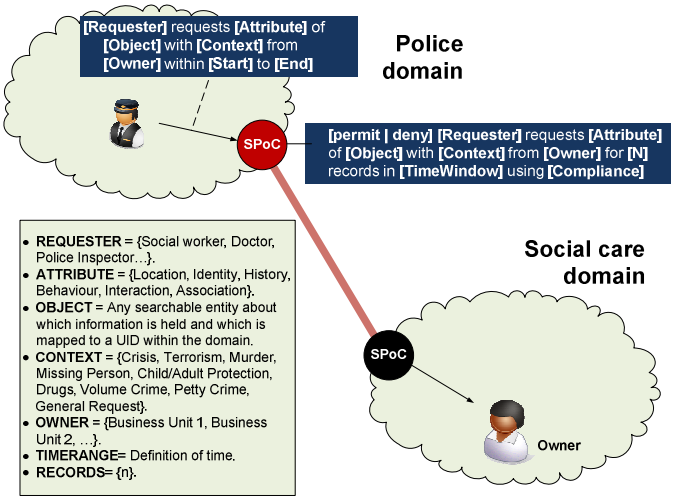

Figure 2: Overview of request and policy implementation syntax

Adding key security elements to this structure yields the proposed syntax for policy rules which are applied into the SPoC:

[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]

A similar matching syntax can then be applied to the request messages:

[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]

Elements of this syntax are defined as:

- **[permit | deny]** This part of the rule syntax indicates the action of the rule and defines whether a message meeting the rule criteria will be permitted or denied.
- **Requester** This identifies an exposed role defined in the ISA. For example, this role might be General Practitioner (FAMDOC) in Primary healthcare (HCP) or a Detective Con-stable (DETCST) in Police services (POL) domain.
- **Object**. This refers to any entity about which information is held, including people, vehicles, events and so on. It is a free-form field.
- **Attribute**. This is a unit of information describing an Object. Attributes may

include details about location (address, mobile phone tracking), identity (name, insurance number), history (prior convictions, documented allegations), behaviour (calm, violent) and association (group memberships, known associates).

- **Context**. This identifies the reason why the information is being shared. The context also governs the level of access and permissions associated with information exchange and, hence, affects the priority accorded to information requests. For example, the Emergency context signifies a threat to life or threat of violence and will require a higher priority allocation than a Vandalism context.
- **Owner**. Defines a role with sufficient privileges to manage all aspects of an information element. The owner has the authority to allow or deny access to an information element, as required by legislation and defined responsibilities. Use of the term owner in this context implies custodianship.
- **[N]** records in **[TimeWindow]** This is a part of the rule syntax that defines the number of records permitted over a period of time, where [N] can be any positive integer, and[TimeWindow] uses the ISO 8601 Coordinated Universal Time (UTC) format (PYYYY-MM-DDThh:mm:ss). In practice, it prevents fishing expeditions
- **[Compliance]** This is part of the rule syntax that refers to policies and legislative requirements that affect the exchange of information. Such as the Data Protection Act, the Human Rights Act, the Freedom of Information Act, and so on.
- **[Start]** This is part of the request that identifies the start of the date/time period over which sharing is requested, such as for ISO 8601 (UTC) standard.
- **[End]** This is part of the request that identifies the end of the date/time period over which sharing is requested

3.4. Context

A key novelty in the proposed system is the use of context for a request, where the ISA will define rights based on the context of the request. For example the rights to data will be higher within the context of a missing persons query than for a trivial access to data. It is thus important that the context levels, and associated rights, are clearly defined in the ISA. For our approach, we developed a conceptual hierarchy loosely based on the categories found in the codified, and hence highly conceptual, German Criminal law. In addition, we use as a proxy to weight severity within a category (e.g. murder vs manslaughter as "offences against the person") the minimum punishment that the crime carries [12]. We are in the process of refining this metric though a questionnaire based approach, that asks key stakeholder to rank different offences according to their severity. This additional measure will help us to model one of the main problems in interagency collaboration, diverging value systems that shape professional cultures.

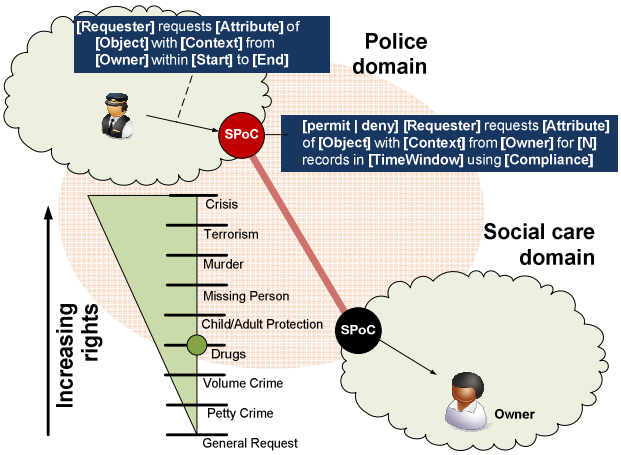

Figure 3: Context definition

3.5. Example

Rules may be used to explicitly permit or deny information exchange requests made by an exposed role. For example, a Senior Family Physician (Requester role=FAMDOCSEN) in Primary healthcare (Requester domain=HCP) is allowed to request a person's medical test results (attribute=MEDTST), from a Laboratory (Owner organisational Sub-unit=LAB) located in a Hospital (Owner organisational unit=HOSP) in Secondary healthcare (Owner domain=HCS), where the person (Object=PERSON) is a patient (Context=PATIENT). A Junior Family Physician (FAMDOCJUN) role from the same domain is not allowed to request this information. These information exchange policies can be used to derive an explicit permit rule (Rule 1) for the FAMDOCSEN role and an explicit deny rule (Rule 2) for the FAMDOCJUN role. These rules would be defined in the Information-Sharing Agreement (ISA) and processed by the SPoC agent (where [PERSON] will be the free-form search field):

Rule 1: [permit] [HCP.FAMDOCSEN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] for [N] records in [TimeWindow] using [Compliance]

Rule 2: [deny] [HCP.FAMDOCJUN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] for [N] records in [TimeWindow] using [Compliance]

Given the above rules, the following requests may be considered:

Req. 1: [HCP.FAMDOCSEN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] within [Start] to [End]

Req. 2: [HCP.FAMDOCJUN] requests [MEDTST] of [PERSON] with [PATIENT] from [HCS.HOSP.LAB] within [Start] to [End]

Thus, a request made by a Senior Family Physician (Request 1) would match Rule 1 and be permit-ted by the SPoC agent. A similar request made by a Junior Family Physician (Request 2) would match Rule 2 and be denied by the SPoC. In the case of Request 2, the SPoC may return the following message:

Junior Family Physician role does not have permission to access the requested resource.

The context of a request for information exchange affects how the request is handled. For example, a Detective Constable (Requester role=DETCST) in the Domestic Violence (Requester organisational unit=DOM) area in Police services (Requester domain=POL) is allowed to request a person's (Object=PERSON) behaviour information (Attribute= BEHAVIOUR) from the Rehabilitation Support organisation (Owner organisational unit=REHAB) in Social Services (Owner domain=SOC), if this is in relation to a domestic violence investigation (Context=DOM.INVST). This following rule may be derived from this policy:

Rule 3: [permit] [POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [DOM.INVST] from [SOC.REHAB] for [N] records in [TimeWindow] using [Compliance]

Thus, the following request, Request 3, made by a Detective Constable would match Rule 3 and be permitted by the SPoC:

Request 3: [POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [DOM.INVST] from [SOC.REHAB] within [Start] to [End]

However, if the Detective Constable requested this information in relation to a vehicle parking offence (Context=VPO), as in Request 4, the request would not match a defined rule and be denied by the SPoC.

Request 4: [POL.DOM.DETCST] requests [BEHAVIOUR] of [PERSON] with [VPO] from [SOC.REHAB] within [Start] to [End]

In this case, the SPoC may return the following message:

Vehicle Parking Offence is not a defined role in Information-Sharing Agreement.

4. Conclusions

The proposed syntax for information exchange builds upon the best practice principles of the Scottish Police, as outlined in the guidance on the Management of Police Information (MoPI), and incorporates formal data sharing rules as specified in Information-Sharing Agreements (ISAs). It uses a modified concept of SPoC agents that use rules derived from organisational policies and legislative requirements to manage information exchange between partner domains. Thus, the proposed syntax offers a mechanism to automate the information exchange process which integrates

with existing systems and policies. SPoC agents ensure compliance with legislation and domain policies and integration with workflow of the roles involved. Currently work is being undertaken on defining use-cases for the interchange of information between the social care and the police domains, as these are possible easier domains to define information exchange. The aim is to show that effective interchange can occur, while using the context field to clearly define the requirements for escalated rights to information. This exchange can thus exist without actually revealing the structure of the databases in each domain, where developers in the domain only require to match the information request syntax formats (as defined within the ISA) to requests for data on their databases. We are also currently refining the metric that underpins the "balancing process" of data protection through a survey based approach. Ultimately, the system should perform three separate yet related functions: a) Permit only Data Protection compliant information exchange; b) create automatic audit trails, so that any abuse of the system (e.g. labeling a minor offence as a murder) can be traced; c) be robust enough to function as a legally valid justification for data sharing. For this, it is necessary top prove abstractly tat only law compliant interactions are permitted by the system .For this purpose in particular, incorporating an explicit representation of legal concepts along the lines Sartor [2] proposes seems to be particularly promising and close to the balancing process of competing interests that is at the core of this approach.

5. References

[1] Lessig, L., *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999

[2] Sartor, G., Doing justice to rights and values: teleological reasoning and proportionality, *Artificial Intelligence and Law* Volume 18, Number 2, 175-215

[3] Gelati, J., Rotolo, A., Sartor, G. & Governatori, G., Normative Autonomy and Normative Co-Ordination: Declarative Power, Representation, and Mandate. *Artificial Intelligence and Law* 12 2004

[4] Police and Crime Standards Directorate (PCSD) and Home Office 'Delivering safer communities: A guide to effective partnership working', Home Office Publications 2007

[5] Clarence, E. & Painter, C., 'Public services under new labour: collaborative discourse and local networking', *Public Policy and Administration* 13(1998) 8–22

[6] Hudson, B., Hardy, B., Henwood, M. & Wistow, G., 'In pursuit of inter-agency collaboration in the public sector: what is the contribution of theory and research?', *Public Management* 1(1999), 235–260

[7] Willem, A. & Buelens, M., 'Knowledge sharing in public sector organizations: The effect of organizational characteristics on interdepartmental knowledge sharing', *Journal of Public Administration Research and Theory* 17(4) (2007), 581–606

[8] Richardson, S., Asthana, S., Inter-agency Information Sharing in Health and Social Care Services: The Role of Professional Culture, *Br J Soc Work)* 36 (4) (2006), 657-669

[9] Daley, D. M. 'Interdisciplinary problems and agency boundaries: Exploring effective cross-agency collaboration', *Journal of Public Administration Research and Theory* 19(3) (2009), 477–493

[10] Association of Chief Police Officers in Scotland (ACPOS) (2008), 'ACPOS Guidance on The Management of Police Information', The ACPOS NIM Development Project

[11] Thomas, R. & Walport, M. (2008), Data Sharing Review Report, UK Ministry of Justice

[12] Kwan Y. K., Chiu L. L., and W. C. Ip, "Measuring Crime Seriousness Perceptions: Methods and Demonstration," in *Criminology Research Focus*, K. T. Froeling, Ed., 2007