Interagency data exchange protocols as computational data protection law.

William BUCHANANa, Lu FANA, Alistair LAWSONa, Burkhard SCHAFAERb1, DS Russell SCOTT, Christoph THUEMMLER, Omair UTHMANIA

a Edinburgh Napier University, Dept. of Computing
b University of Edinburgh, School of Law, c Scottish Police College, 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.

From MoPls to software code

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 life or property. Put simply, it is more acceptable to invade the privacy of a person under reasonable suspicion to plan a terrorist attack than to investigate a littering offence. Of course, today most of the relevant data is stored electronically, and information exchange requests will also be transmitted using ICTs. Larry Lessig [1] popularized the idea that on the internet, regulation through laws is often inefficient, but embedding legal concepts directly into the code is a feasible alternative. Similarly, rather than 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, develops data exchange protocols that 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.

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 and secondary healthcare; Social Services; Education; and Fire and Rescue services. Such requests typically form the basis for information-sharing agreements between the police and their community partners. The application of policy definitions using rules within these ISAs can be seen as analogous to 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. 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 based policing, focuses on community actions. Here measures are taken to minimise future, yet unspecified criminal activities through e.g. citizen advice activities. Level 2, preventative intervention, focuses on prevention of specific, identified criminal activities, where the requirement to share information will often depend on the seriousness of anticipated harm. Level 3, Crime investigation, deals with the investigation of a specific crime. Unlike Level 2, which is forward looking, Level 3 is backwards looking, a singular past event is the focus, the main harm has already occurred. Level 4, focuses on analyzing 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 syntax 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). ISAs define the agreed specific rules, derived from policies, that direct the recording, access, review and dissemination of information between partner agencies. 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. The function of these SPoC agents is similar to firewalls within a computer network. At a basic level, firewalls use a defined set of rules to either permit or deny network 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 a rule from the set of rules in the ISA. If the request does not match a given rule, the agent will then attempt 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.

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. 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. All of the other fields within the rules are then used to match the request. Adding key security elements to this structure yields the proposed syntax for policy rules which are applied into the SPoC:

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

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

\[
[\text{Requester}] \ requests \ [\text{Attribute}] \ of \ [\text{Object}] \ with \ [\text{Context}] \ from \ [\text{Owner}] \ within \ [\text{Start}] \ to \ [\text{End}] \\
\]

A key novelty in the proposed system is the use of context for a request, where the ISA defines 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 [2]. 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=FAMDOCSN) 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 (FAMDOCSN) 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 FAMDOCSN role and an explicit deny rule (Rule 2) for the FAMDOCSN role:


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


Thus, a request made by a Senior Family Physician (Request 1) would match Rule 1 and be permitted 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.**

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. 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.

**References**