Evidence-Based Solution to Information Sharing between Criminal Justice Agencies[1]

Darryl Plecas, Amanda V. McCormick, Jason Levine, Patrick Neal, & Irwin M. Cohen

Author Information

Dr. Darryl Plecas
Darryl.Plecas@ufv.ca 604-504-7441
School of Criminology and Criminal Justice
University of the Fraser Valley
33844 King Road
Abbotsford, B.C.
V2S 7M8 Canada

Dr. Plecas is the RCMP University Research Chair and Director of the Centre for Criminal Justice Research at the University of the Fraser Valley (UFV). His research interests primarily concern crime reduction, prolific offenders, and police operations.

Amanda V. McCormick, M.A.
Amanda.McCormick@ufv.ca 604-504-7441
School of Criminology and Criminal Justice
University of the Fraser Valley
33844 King Road
Abbotsford, B.C.
V2S 7M8 Canada

Amanda McCormick is professor in the School of Criminology and Criminal Justice at the University of the Fraser Valley, and the Research Coordinator with the British Columbia Centre for Social Responsibility. Her research interests primarily concern policing, young offenders, mental health and personality issues, and fire prevention. She is currently completing her doctorate in the school of Criminology at Simon Fraser University; her dissertation concerns serious and violent young offenders.

[1] This paper originates from a project done for and with the assistance of the Operations Strategy Branch, E Division, Royal Canadian Mounted Police.

Jason Levine, B.A.
Jason.Levine@rcmp-grc.gc.ca 604-928-4743
Operations and Strategy Branch
Royal Canadian Mounted Police
4949 Heather Street
Vancouver, B.C.
V5Z 1K6 Canada

Jason Levine has recently graduated from the University of the Fraser Valley and is currently employed by the Royal Canadian Mounted Police. His research interests are in criminal network analysis, major crimes, and justice and public safety data quality assurance. He is currently the Assistant Lab Manager for the Centre for Criminal Justice Research.

Patrick Neal, M.A.
Patrick.Neal@ufv.ca 604-504-7441
School of Criminology and Criminal Justice
University of the Fraser Valley
33844 King Road
Abbotsford, B.C.
V2S 7M8 Canada

Patrick Neal is the Centre for Criminal Justice Research Lab Manager in the School of Criminology and Criminal Justice in the University of the Fraser Valley. He has also been the Research Information Manager for the British Columbia Centre for Social Responsibility. His research interests include knowledge management, open source intelligence operations, systems theory, and information quality assurance models.

Dr. Irwin M. Cohen
Irwin.Cohen@ufv.ca 604-504-7441
School of Criminology and Criminal Justice
University of the Fraser Valley
33844 King Road
Abbotsford, B.C.
V2S 7M8 Canada

Irwin M. Cohen is a professor at the School of Criminology and Criminal Justice in the University of the Fraser Valley, and the Research Director with the British Columbia Centre for Social Responsibility. His research interests primarily concern policing, young offenders, terrorism, and Aboriginal issues.

Evidence-Based Solution to Information Sharing between Criminal Justice Agencies

Abstract

The aim of this study was to test a technological solution to two traditional limitations of information sharing between criminal justice agencies: data quality and privacy concerns. Entity Analytics Software (EAS) was tested in two studies with North American criminal justice agencies. In the first test, duplicated cases held in a police record system were successfully identified (4.0%) to a greater extent than the traditionally used software program (1.5%). This resulted in a difference of 11,954 cases that otherwise would not have been identified as duplications. In the second test, entity information held separately by police and border officials was shared anonymously between these two organizations. This resulted in 1,827 alerts regarding entities that appeared in both systems; traditionally, this information could not have been shared, given privacy concerns, and neither criminal justice agency would be aware of the relevant information held by the other. Data duplication resulted in an additional 1,041 alerts, which highlights the need to use technological solutions to improve data quality prior to and during information sharing. While only one potential technological solution (EAS) was tested and organizations must consider the potential expense associated with implementing such technology, the implications resulting from both studies for improved awareness and greater efficiency support and facilitate information sharing between criminal justice organizations.

Keywords: Information Sharing, Technological Solution, Criminal Justice Agencies

Categorization: Research Paper

1. Introduction

Information sharing in the field of criminal justice involves collecting and organizing facts and figures (i.e. data), giving context to the data, and providing the information to various other individuals and/or organizations for strategic and operational decision making. For example, to be most effective and efficient, police agencies must share information, not only with other police agencies, but also with other organizations, such as customs agencies, the courts, mental health systems, corrections, and researchers, academics, and policymakers. Furthermore, to be most effective, information should be shared both locally and across jurisdictions, including international exchanges of information. When this information is accurate, error-free, concise, usable, and consistent (e.g. Zhu and Wang, 2008; Kahn et al., 2002), there are multiple benefits to this exchange, including avoidance of data collection duplication and better decision making. Moreover, information sharing can also maximize the use of limited resources (Fraser and Stoddart, 2009; National Strategy for Neighbourhood Renewal, 2000; Dawes, 1996), timely awareness and greater understanding of the full scale of the situation (Tyworth and Sawyer, 2006; NASIRE, 2000), the ability to develop integrated approaches based on information taken from multiple sources (Landsbergen and Wolken, 2001), and greater productivity (Zaworski, 2005).

Yet, the sharing of information has been a long-standing challenge for a variety of reasons, including privacy concerns (Landsbergen and Wolken, 2001), competitiveness between individuals and/or organizations (Brewer, 2008), inter and extra organizational mistrust (e.g. Tyworth, 2009; Tyworth and Sawyer, 2006; Drake et al., 2004; National Strategy for Neighbourhood Renewal, 2000; Dawes, 1996), and technological issues (Tyworth and Sawyer,

2006; Ministère de la Justice de Québec[2], 2003; Landsbergen and Wolken, 2001). However, there are recent developments in the field of information sharing that demonstrate the ability of different agencies to successfully share critical and sensitive information.

This article will review existing examples of information sharing systems utilized in North America. In addition, it will provide the results of a successful information sharing study between two criminal justice agencies in Canada. Specifically, the system reviewed in the current study responds to two key issues concerning information sharing; namely, data quality and privacy. The benefits, limitations, and policy implications of this process will also be discussed.

2. Literature Review

The challenges to information sharing can be summarized with reference to four key problems: (1) privacy; (2) competitiveness; (3) quality of information sharing; and (4) technology. The concern over privacy stems from legal guidelines designed to protect the confidentiality of citizens' information and prevent unauthorized access or use to this information. Given this, any system of information sharing must perform within the confines of such legislation; in Canada, this involves the federal *Privacy Act* (Fraser and Stoddart, 2009). The *Privacy Act* mandates the type of information that can be collected by various agencies and organizations, and provides regulations regarding the holding and sharing of that information. In effect, the personal information of individuals must be protected from loss or disclosure that falls outside the regulations, and there must be a legislative authority to collect that information (Fraser and Stoddart, 2009). However, while the *Privacy Act* intends to prevent unauthorized access to or use of confidential data, it can also contribute to confusion regarding information

[2] Hereafter Quebec, 2003

sharing protocols; specifically, what information can be shared, with whom, and how can it be protected during the sharing process. This may result in one agency (e.g. Border Services) failing to share the names of individuals in their database with other agencies (e.g. police) who hold additional relevant information about the same individuals; together, these pieces of information could provide a more complete picture that would enable criminal justice agencies to determine a more accurate risk assessment profile, yet privacy concerns may prohibit this from formally occurring.

Competitiveness between those who own the data can also contributes to the prevention of information sharing. For instance, LeBeuf and Pare (2005) found that, in spite of having technology that could securely transmit confidential data, one-third of Canadian police officers did not share information with non-police officers, even when the legal guidelines of information sharing allowed them to. Yet, for information sharing to work successfully, each stakeholder in the system must be willing to collaborate in providing their information to others. However, as many organizations tend to be resistant to change, developing an information sharing system often involves modifications to organizational culture and identity (Tyworth, 2009; Quebec, 2003). For the purposes of this paper, organizational identity reflects the unique characteristics and values inherent to a particular organization (Tyworth, 2009). Thus, each individual agency involved in an information sharing capacity tends to operate under "its own leadership, management structure, norms, rules and regulations, missions, and ... infrastructures" (Tyworth, 2009: 2) which can lead to competitiveness and unwillingness to share information with another organization or agency.

This is particularly true of the United States, where each state exerts a substantial amount of independent control over their local criminal justice system, resulting in a wide variety of

organization-specific values, cultures, and practices that render information sharing across jurisdictions a difficult and tedious practice (Tyworth and Sawyer, 2006). As an example of the process needed to overcome organizational culture and traditional practices, in San Diego, California, the development of an integrated criminal justice information sharing system required the construction of a governance structure to promote inter-agency collaboration and to break down the competitive barriers that previously prevented the sharing of information (Tyworth and Sawyer, 2006). In particular, their focus was on the challenges involved in designing a workable system that met the needs, values, and cultures of the various organizations served.

The final two challenges to information sharing reflect technological limitations. Firstly, different agencies, even within the same field, may use inconsistent and incompatible technological platforms to collect and host their information (Quebec, 2003). In effect, many information systems are simply outdated; therefore, to suit the needs of an organization, additional programs or systems may be developed in-house to achieve the outcomes not met by older systems. In contrast, other organizations may use a more technologically advanced single system that is capable of holding vast amounts of information (Quebec, 2003). Overcoming the challenges of sharing information between different programs, especially among those that lack standardized processes, can become costly and overwhelming (Quebec, 2003). Similarly, as a result of technological differences, in addition to the aforementioned differences in organizational values and practices, the way in which each organization manages and shares its data may differ, increasing the difficulty of successful information sharing and integration (Quebec, 2003).

The second technological concern is based on the possibility that when information is shared between agencies, there is a risk of information duplication or loss. Again, this concern

arises because of the varying quality of data contained within each organization's system (Quebec, 2003). In effect, systems that contain identifying information on individuals may record similar information differently (Fraser and Stoddart, 2009). Furthermore, information may be entered incompletely or incorrectly. For instance, while a court database may hold updated information on the address of an individual, a police database may hold an old and no longer applicable address. Similarly, the full name of an individual may be found in both systems, but spelled incorrectly or differently in one system. Alternatively, name changes (such as changes as a result of marriage) may be updated in one database, but not in another. Given this, when an attempt is made to merge the information on an individual, the system may recognize one person as two distinct individuals and their records will be duplicated, resulting in two individuals rather than one single entity.

Information duplication can also result from the strict adherence to protect privacy. As there are often no federal guidelines in place for how information can be shared, instead there are typically guidelines that stipulate who can access what information and how it must be protected, individual agreements may be drafted between two or more agencies that provide for information sharing within the guidelines of the federal privacy legislation. For instance, Fraser and Stoddard (2009) identified more than 60 individual agreements between Canadian federal agencies and their partners regarding sharing and validating of information. However, these agreements were often unilateral, in that the agreement stipulated for data to be provided from one institution to another, rather than a mutual sharing of information. Further, many of these agreements did not include a process for data validation or correction; therefore, if the information shared from one institution to another was subsequently determined by the receiver to be less accurate than information coming from a third party (i.e. another partner or the individual themselves), the

agreements did not provide a standardized process whereby the receiver could update the initial provider of information on their now inaccurate data (Fraser and Stoddard, 2009).

A second concern with regards to data quality is the potential for inaccurate data. Chen and colleagues (2003) identified that criminal offenders frequently provided police with inaccurate identification information, including their name, the accurate spelling of their name, their date of birth, and/or their current address. Police may not have the resources or the ability to ensure that all of the information they collected was accurate and not an alias or a direct fabrication. Thus, when they share this information with other agencies, it can result in duplicated records of a single individual with slightly different information reflected in each entry. In other words, the quality of the information that is shared is a major concern for those using the data as it may result in duplication errors, duplicated processes, and inaccurate data. As such, there is a need for a way to determine whether two different entities or data entries are, in fact, the same individual.

This need led to the development of Identity Resolution; a concept that reflects a technological process whereby identifying information is compared and decisions are made using a set of pre-defined rules about data accuracy to identify and resolve duplicate entries (Bloor and Halper, 2006). For instance, similar names may be compared and entities may be merged on the basis of additional matching information; thus, two entities with a similar name may be merged on the basis of also sharing a birth date and/or address (Bloor and Halper, 2006).

2.1 Examples of Information Sharing Systems

There are longstanding challenges that threaten the development of information sharing. However, recent innovations may assist in solving one or some of these challenges. Since 2003, British Columbia has utilized the Police Records Information Management Environment

(PRIME-BC) to share information between a variety of police agencies, including the federal Royal Canadian Mounted Police who are contracted individually by cities in British Columbia to provide police services, and municipal agencies, such as the Abbotsford Police Department (APD) or the Vancouver Police Department (VPD). Traditionally, such information could not be shared given the different technological platforms for collecting and holding information used by these organizations, as well as due to jurisdictional boundaries. Therefore, when police needed information on a person of interest, they were not necessarily able to access information given that they may not have known whether additional information was available, and if so, where that information was held (Brewer, 2008). Furthermore, access to information would not be timely, as police were unable to retrieve such information while in their patrol car (Brewer, 2008). In fact, many reports that would be useful to police would originally be filled out on paper, potentially taking months before entry into a computer system could be completed (Brewer, 2008).

As a result of the lack of information sharing, the British Columbia Chiefs of Police pushed for the creation of a single information sharing platform - PRIME. Since the development of this system, information has routinely been shared among police agencies in British Columbia and is done so in a timely fashion. In effect, PRIME-BC is now accessible on more than 2,000 mobile work stations (i.e. patrol car computers) and is used by all British Columbian police officers, regardless of organization or jurisdiction.

Information is initially recorded on PRIME by a police dispatcher or police officer, with subsequent entries made to correct or update the information (Brewer, 2008). Collected information may include, but is not limited to, name, date of birth, gender, ethnicity, criminal history, history of contact with police, and/or mental health issues known to police. Further, a

picture of the person of interest may also be available. In addition, police can now query multiple databases across jurisdictions with a single entity query, including the Canadian Police Information Centre (CPIC), Police Information Records System (PIRS), PRIME, Canadian Firearms Agency, and the Police Information Portal. Once the information has been entered, it is reviewed for quality and subsequently becomes part of the record management system (Brewer, 2008).

Despite efforts at data quality control, PRIME-BC has recently been criticized for errors involving missing data and data duplication. There is particular concern with the matter of duplicate name entries in the Master Name Index (MNI). When police search for information on a person of interest, such as history of violence, mental health issues, or the presence of a criminal record, they do so using the MNI. However, some individuals may have the same or similar first and last names (Bloor and Halper, 2006), and police may not know which information is relevant to the current situation. Alternatively, a name may not appear in the MNI given that the offender provided inaccurate information either in the current or a previous situation (intentionally or not), and a match is not made in the database. For instance, Bloor and Halper suggested that "David Jones, David R. Jones, and David Jones Jr. may all refer to the same person, but be recorded differently simply because different data entry forms are used" (2006: 2). Thus, when police search for *David R. Jones*, the MNI will reflect entries for three or more individuals and the police will need to determine whether this is a single entity whose information has been duplicated or whether these are separate entities.

In 2003, the province of Quebec began to develop the Integrated Justice Information System within which stakeholders, such as the police and Attorney-General prosecutors, could electronically share information on criminal justice system clients (Quebec, 2003). The logic

behind the development of this system was that the current system of sharing paper-stored information was inefficient. Not only were paper records of varying quality, but they were infrequently shared in a timely manner, resulting in a delayed flow of information to justice system stakeholders (Quebec, 2003). As a result, the province developed a computer based information sharing program composed of a variety of applications supporting the unique needs of each of the system stakeholders (Quebec, 2003). For instance, applications allowed for police to create and submit electronic records to the Attorney-General prosecutors, who could likewise share this information with the police and the court. This resulted in an improved flow of information, reduced administrated costs, and greater public safety due to the rapidity of information sharing and subsequent use of information by stakeholders (Quebec, 2003). Simultaneously, the system protected the privacy of information by operating within the confines of privacy legislation (Quebec, 2003).

A second example can be found in the Automated Regional Justice Information System (ARJIS) in San Diego (Tyworth and Sawyer, 2006). Similar to the Quebec integrated system, the development of ARJIS was driven by the need to improve efficient communication of information between a variety of state justice agencies and organizations. The technological aspect of this system involved merging ten information systems now simultaneously utilized by a variety of justice organizations and agencies in San Diego, including several police agencies and border patrol (Tyworth, 2009; Tyworth and Sawyer, 2006). In effect, this system connects county, state, and federal stakeholders. According to a recent study, on a daily basis, the system handles “over 35,000 transactions accessing 2.9 million recorded incidents, 5 million digital photos, and 4.4 million map and crime statistics" (Tyworth and Sawyer, 2006: 4).

In order to respond to the traditional barriers to information sharing, ARJIS involved the development of a Joint Powers Agreement. Each stakeholder essentially joined into a contract whereby they each agreed to support the system. According to Tyworth and Sawyer (2006), this resulted in ARJIS being developed as a shared system that was independent of each organization or agency. ARJIS resulted in the creation of several committees composed of members of each agency who would make decisions about policies and operations; therefore, each competing concern would be addressed and accounted for (Tyworth and Sawyer, 2006). Decisions were to be made under the auspice of improving law enforcement, and the process of sharing information and ensuring data quality would be jointly agreed upon (Tyworth, 2009). However, a more recent review indicated that ARJIS continued to be limited by each individual agency insisting on retaining control over information they have collected and independently providing approval for the use of that information (Tyworth, 2009).

3. Current Study

As previously discussed, concerns over privacy and data duplication are two of the long-standing challenges associated with information sharing. However, recent technological innovations have resulted in a method of information sharing that responds to these two issues. One such method is IBM's Entity Analytics Software (EAS). This software consists of three components: Identity Resolution (IR); Relationship Resolution (RR); and Anonymous Resolution (AR). EAS's IR component merges entities together, while the RR component establishes relationships between these entities. AR allows these processes to be done anonymously, thus avoiding privacy concerns or data security issues regarding potentially highly sensitive information (Bloor and Halper, 2006). Once merged and related in EAS, these entities can be cleanly exported back to the original system, where they can be analyzed and used for

informed decision making. EAS has previously been evaluated in a business setting in which it was concluded that EAS increased the efficiency and accuracy of the information held by a financial institution concerned with global money laundering (Bloor and Halper, 2006). The current study evaluated the applicability of EAS to criminal justice data.

Two separate studies were conducted using EAS. The first test examined whether EAS could identify duplicate cases from PRIME and merge them successfully into one entity. The second test focussed on whether EAS could anonymously merge data with similar entities from two agencies; namely, the police and border service data.

3.1 Test One – EAS and the PRIME System

Acknowledging the need to improve the data quality of PRIME's Master Name Index, the RCMP tested the capability of EAS to find and remove duplicate cases using PRIME data. To this end, EAS was installed on a standalone laptop, and the default resolution rules that came with the Relationship Resolution software were used to identify possible duplicates. These resolution rules established the minimum threshold to identify a duplicate entity, such as a matching name and date of birth or a matching name and unique ID number.

To test the ability of EAS to identify duplicate cases, 478,163 records were extracted from the PRIME System and loaded separately into both EAS and SPSS.[3] Using data matching techniques based on the first name, last name, and date of birth, SPSS identified that 1.5% of the extracted data was duplicated. In contrast, EAS identified 4% of the data as duplicated. This 2.5% difference accounted for a difference in 11,954 records between the two programs and represented a substantial number of records that were not detected by the typical program used by the RCMP. Moreover, the percentage of matched entities in EAS increased with the number

[3] Statistical Package for the Social Sciences (SPSS) is currently used by the RCMP to analyze and provide statistical information about the data being collected.

of records loaded into the system. This is important as the data extract for the initial test represented only a portion of the total number of records currently housed in the PRIME system. In effect, assuming that the percentage continued to increase as the total numbers of records in PRIME are loaded into EAS, a large number of records could be identified as duplicates, even if the percentage eventually levelled off.

The fact that EAS was able to identify a larger than expected number of duplicate entities in the PRIME system suggested that software solutions can address a critical aspect of data quality. While it is true that manually investigating data to determine duplicate cases (as is currently the case with PRIME Transcription units) can reduce the number of duplicate entities and increase data quality, EAS has a demonstrated ability to systematically find duplicate entities on a large scale much more quickly. Critically, the fact that a total of 18,170 people were identified as possible duplicates in a sample of just 478,163 records underlines more than just a resourcing issue; it highlights the substantial effect that data quality issues may have on information sharing.

3.2 Test Two – Information Sharing Between Two Federal Agencies

In the second test, EAS was used by the RCMP and the Canadian Border Services Agency (CBSA) to test how data could be shared in a secure and legal manner. The Anonymous Resolution program (AR) is one part of the EAS suite and offers a systemic method in which data from multiple sources is anonymized and then matched together to determine if two or more agencies have information about the same entity.

The AR software was installed in both an RCMP and CBSA environment. Both the RCMP and the CBSA performed a data extraction from their records system and ran their extracted data through the AR software. Representatives from both agencies physically brought

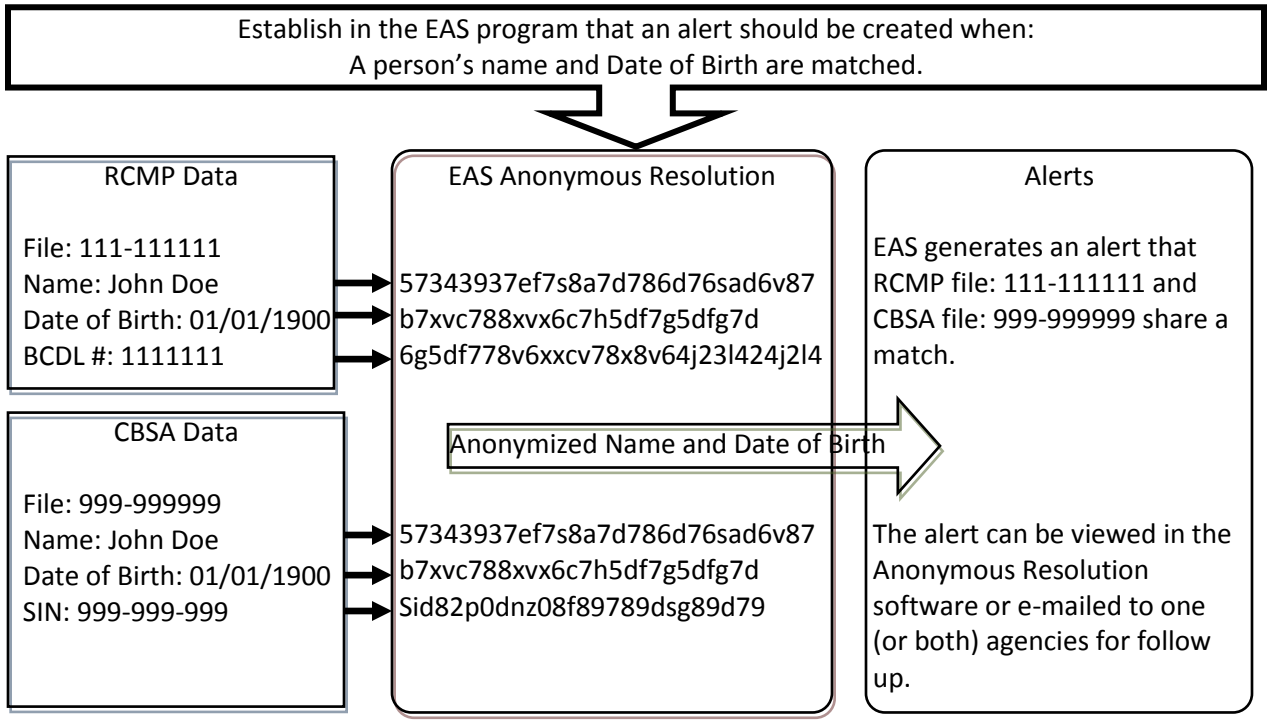
the resulting anonymized data file to a protected environment, where a separate AR package had been installed on a standalone laptop. This Anonymous Resolution package was configured for the following six resolution rules:

1) Name and unique number (i.e. SIN, Driver's License)
2) Name and non-unique number (i.e. phone number)
3) Name and address (no conflicting information)
4) Name, Address, and Generation
5) Name and Date of Birth
6) Identifying attribute only

These rules allowed for six different possibilities in which an alert would be generated. In fact, as the anonymized data files were processed through the Anonymous Resolution software, alerts were instantly generated. In a real life environment, these alerts could be e-mailed to one or both agencies pointing back to the files generated the alert.[4] It is important to stress that at absolutely no time could any data from one agency be read by the other agency; all data was anonymized at the agency level, leaving only the file numbers visible which would allow for subsequent investigations. The entire concept is illustrated in Figure 1.

[4] Due to a test environment, this e-mail function was not needed as the results could be jointly-viewed through the Anonymous Resolution package.

Figure 1: Concept behind EAS Anonymous Resolution



Of the 103,099 RCMP files and 60,562 CBSA files loaded into the Anonymous Resolver, a total of 5,651 alerts were generated. Approximately half of the alerts (2,783) were a result of a shared relationship between two entities (i.e. a family member). The 2,868 remaining alerts involved entities matched between both agencies file numbers. It is worth noting that of these 2,868 entity matches, only 1,827 alerts were attributed to a distinct entity match suggesting that the other 1,041 alerts was generated because of duplicated entities. The fact that 1,041 alerts could be attributed to duplicate entities was not surprising given that only the RCMP used EAS to remove the duplicate entities prior to the anonymization process, while the CBSA files were taken from occurrences as opposed to an equivalent Master Name Index. In effect, the results of this test clearly pointed toward the substantial effect that data quality issues, such as duplicate entities, has when sharing information.

In summary, the 1,827 generated alerts based on a unique individual matching from both RCMP and CBSA files showed a real need to systematically share information between agencies. Analysts from both the RCMP and CBSA were able to confirm that new information would have been available to at least one organization in a majority of these alerted cases. Given this, both agencies agreed that using a software solution, such as EAS, would be of direct benefit.

4. Conclusion

EAS was the main software solution discussed in this article because it was the software package undergoing testing by the RCMP. However, it is important to note that there may be other software solutions that can detect duplicate entities or anonymously share information. Regardless of the solution used, it is critical to actively seek ways to solve the ongoing problems of data quality, duplicate data, and lack of information sharing. As demonstrated in this article, EAS is simply one such viable solution.

Although EAS addresses several of the discussed problems associated with managing the information contained in databases, there are some obstacles that need to be overcome before any software solution to sharing information is widely adopted. For instance, to effectively work with databases requires some understanding of the software and the technical terminology associated with databases. In addition, there is the need to invest in software, such as EAS, which can be very expensive. Further, a recurring problem discussed in the literature and a general theme of this article is the problem of poor data quality. However, data quality is a very broad term that covers a multitude of unique problems. The solutions to these problems vary in complexity and only one of these many problems, namely duplicate entities, is effectively addressed by software such as EAS. Given this, it is necessary to understand that software, such as EAS, is not a ‘data quality tool’ as it does not add/delete data, fix typographical errors, offer

suggestions about formatting data, or provide any number of additional data quality management tools. Still, software, such as EAS, is vital to ensuring that a very important aspect of data quality, namely duplicate entities, can be improved.

Notwithstanding the aforementioned limitations, there are clearly viable technological solutions which can overcome the most commonly referred to obstacles associated with information sharing. While acknowledging the short-term costs associated with purchasing the software and training users, the benefits resulting from improved information sharing have demonstrated the potential to far outweigh these costs in the long-term. Just considering the benefits to public safety and the opportunities that accurate information provides to facilitate multi-agency, proactive criminal justice approaches should be sufficient to justify the widespread implementation of proven technological solutions to information sharing, such as EAS.

References

Bloor, R. & Halper, F. (2006). *The Business Applications of Identity Resolution*. Hurwitz & Associates.

Brewer, B. (2008). PRIME-BC A Canadian RMS Case Study. *Law and Order Magazine, April*. Accessed August 7, 2009 from http://www.hendonpub.com/resources/articlearchive/details.aspx?ID=205877.

Chainey, S. & Smith, C. (2006). Review of GIS-based information sharing systems. *Home Office Online Report 02/06*. Accessed November 22, 2006 from http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0206.pdf.

Chen, H., Chung, W., Qin, Y., Chau, M., Xu, J., Wang, G., et al. (2003). *Crime Data Mining: An Overview and Case Studies.* COPLINK Artificial Intelligence Lab, Department of Management Information Systems, University of Arizona, Tuscon.

Dawes, S.S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*(3): 377-394.

Drake, D.B., Steckler, N.A., & Koch, M.J. (2004). Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures. *Social Science Computer Review, 22*(1): 67-84.

Fraser, S. & Stoddart, J. (2009). *Report of the Auditor General of Canada to the House of Commons: Managing Identity Information*. Office of the Auditor General of Canada.

Kahn, B., Strong, D., & Wang, R. (2002). Information quality benchmarks: Product and service performance. *Communications of the ACM, 45*(4), 184-192.

Landsbergen, D. Jr. & Wolken, G. Jr. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. *Public Administration Review, 61*(2): 206-220.

LeBeuf, M. & Pare, S. (2005). Police information sharing in Canada: Balancing security, efficiency, and collaboration. *Research and Evaluation Branch (RCMP).* Ottawa, ON.

National Strategy for Neighbourhood Renewal. (2000). *Report of the Policy Action Team 18: Better Information.*

Ministère de la Justice de Québec. (2003). *Preliminary Analysis of the Integrated Justice Information System (IJIS): Executive Summary*.

Tyworth, M. (2009). Institutional and organizational influences on the design of Integrated Criminal Justice Information Systems. *Paper presented at the 4th Annual iConference.* Accessed October 2009 from http://nora.lis.uiuc.edu/images/iConferences/mtyworth_final1.pdf.

Tyworth, M. & Sawyer, S. (2006). Integrated Criminal Justice System Design: Designing an appropriate governance structure. In B. Van de Walle and M. Turoff (eds.), *Proceedings of the 3rd International ISCRAM Conference*. Newark, N.J.

Zaworski, M.J. (2005). *An Assessment of an Information Sharing Technology (ARJIS): Examining its Potential Contribution to Improved Performance through the Eyes of Street Level Officers.* Research Report submitted to the U.S. Department of Justice.

Zhu, H. & Wang, R. (2008). An information quality framework for verifiable intelligence products. In Y. Chan et al. (eds), *Data Engineering: Mining, Information, and Intelligence.* New York, NY: Springer.