Chapter 11

THE PARTNERSHIP AND COLLABORATION FRAMEWORK

Chapter Overview

ISI research requires a close partnership between academic researchers and agency practitioners. Researchers would benefit from the testbed and inputs provided by domain experts. On the other hand, law enforcement and intelligence practitioners could leverage advanced information technologies for their works. However, developing a win-win relationship is not always easy. Agencies often have a pressing and immediate need that cannot wait for long-term, academic research. Data confidentiality concerns may often create barriers for collaboration. In this chapter we present selected research collaboration challenges facing ISI researchers and describe our COPLINK project experience in addressing these challenges. In particular, we present samples of a user data license and Memorandum of Understanding (MOU) that are useful for national security research and collaboration partnership.

11.1 Introduction

To accomplish the six critical mission areas of national security the Department of Homeland Security has proposed to establish a network of laboratories consisting of satellite research centers of excellence across the nation. The purpose is to create a multidisciplinary environment for developing technologies to counter various threats to homeland security. However, information sharing and collaboration across different jurisdictions, agencies, and research institutes is not merely a technical issue. A variety of social, organizational, and political barriers need to addressed, including:

- *Security and confidentiality*. In the intelligence and law enforcement domain, security is of great concern. Data regarding crimes, criminals, terrorist organizations, and potential terrorist attacks may be highly sensitive and confidential. Improper use of data could lead to fatal consequences.
- *Trust and willingness to share information*. Different agencies may not be motivated to share information and collaborate if there is no immediate gain. They may also fear that information being shared would be misused, resulting in legal liabilities.
- *Data ownership and access control*. Who owns a particular dataset? Who is allowed to access, aggregate, or input data? Who owns the derivative data (knowledge)? For both original and derivative data, who is allowed to distribute them to whom?

As a leading research center for law enforcement and intelligence information and knowledge management, the NSF COPLINK Center at the Artificial Intelligence (AI) Lab of the University of Arizona is intended to become a part of the national network of ISI research laboratories. During its development over the past decade the COPLINK Center has encountered many of these non-technical challenges in its partnerships with various law enforcement and federal agencies. We present some of our experiences and lessons learned in this section.

11.2 Ensuring Data Security and Confidentiality

In any information sharing initiative, it is essential to make sure that the data shared between agencies is secure and that the privacy of individuals is respected. In our research we have taken the necessary measures to ensure data privacy, security, and confidentiality. Data shared between law enforcement agencies, such as the Tucson Police Department (TPD),

Phoenix Police Department (PPD), and Tucson Customs and Border Patrol (CBP), contained only law enforcement data and was available only to individuals screened by these agencies using a combination of TPD Background Check, Employee Non-Disclosure Agreement (NDA), and the Terminal Operator Certificate (TOC) test.

All personnel who have access to law enforcement data fill out background forms provided by TPD and have their fingerprints taken at TPD. They also sign a non-disclosure agreement provided by TPD. In addition, they take the TOC test every year. The background information and fingerprints are then checked by TPD investigators to ensure lack of involvement in criminal activity and for verification of identity.

In addition to the above forms and test, all law enforcement data in the University of Arizona's COPLINK Center reside behind a firewall and in a secure room accessible only by activated cards to those who have met the above security criteria. As soon as an employee stops working on projects related to law enforcement data, their card is de-activated. However, the NDA is perpetual and remains in effect even after a researcher or employee leaves. Such requirements are similar to those imposed upon non-commissioned civilian personnel in a police department.

A sample individual user data license agreement is shown in Figure 11-1. The sample document was developed by university contracting officers and lawyers in several institutions and government agencies. Most of the terms and conditions are applicable to national security projects that demand confidentiality.

11.3 Reaching Agreements among Partners

Federal, state, and local regulations require that agreements between agencies within their respective jurisdictions receive advance approval from their governing hierarchy. This precludes informal information sharing agreements between those agencies. We found that requirements varied from agency to agency according to the statutes by which they were governed.

For instance, the ordinances governing information sharing by the city of Tucson varied somewhat from those governing the city of Phoenix. This necessitated numerous attempts and passes at proposed documents by each city's law enforcement and legal staff before a final draft could be settled upon for approval by the city councils.

We found in general that similar language existed in the ordinances and statutes governing this exchange but the process varied significantly.

The [Agency] hereby grants access to the [Designated Data] data to the individual named below, hereinafter Licensee: [Name] [Organization] [Official mail address] [Telephone] [Facsimile] [Email]; subject to the following understandings, terms and conditions. These understandings, terms and conditions apply equally to all or to part of the data.

Permitted Uses:

- The information may only be used for research and development as described in the [Proposal Name] project (hereinafter referred to as *the proposal*).
- Summaries, analyses and interpretations of the properties of the data may be derived and used for research and development purposes.
- No excerpts of the data may be published in any context, or displayed to others except other Licensees with a signed Individual User Data License on file at [Agency] also bearing research and development responsibilities for the project described in the proposal.

Access to the Information:

- Access to the data is granted solely to the Licensee listed above for purposes of discharging his or her responsibilities of carrying out the research and development work described in the proposal.
- This license does not extend to other individuals within the Licensee's organization.
- The access is to be terminated on [End Date].

Indemnification:

- [Agency] shall not be liable in any way to the Licensee for any delays, inaccuracies, errors or omissions therefrom or in transmission or delivery of all or any part thereof or for any damages arising therefrom or occasioned thereby.
- In no event shall [Agency] be liable for any direct consequential, punitive, special or any other damages arising in any way from the availability of the service regardless of the form of action, whether contract or tort.

Delivery and Acceptance:

- Upon Licensee's execution of this Agreement, [Agency] shall deliver the data to Licensee.
- Licensee acknowledges and agrees that the data is licensed on an ``as is with all defects'' basis and is provided without maintenance, support or improvements. Accordingly, [Agency] shall not be required to make any corrections, or provide maintenance, or provide updates to Licensee, or assist Licensee in the understanding or use of the Database. No guarantee is made that the dictionary is adequately or completely described in the documentation.
- If [Agency] makes corrections or provides maintenance or updates to the data, [Agency] shall offer such corrections, maintenance and/or updates to Licensee.

Signed this __ day of ___, 20__ _____ (Licensee)

Figure 11-1. A Sample Individual User Data License.

Between [AGENCY 1] and [AGENCY 2]

WHEREAS, the real-time sharing of data and the development of tools may be essential for partners and for agencies and scientists who can assist in the development of such tools; and

WHEREAS, such interoperable multi-disciplinary data systems must incorporate appropriate protections to maintain confidentiality and scientific integrity of the data; and

Now therefore the parties hereto agree as follows:

I. [AGENCY 1] and [AGENCY 2] will use collaborative efforts to develop a prototype model interoperable data system.

II. [AGENCY 1] and [AGENCY 2] will share data as permitted by the law of each state, respectively.

III. [AGENCY 1] and [AGENCY 2] will continue their current testing systems unless changes are required for state purposes.

IV. All parties shall own the data system design generated under this MOU subject to the rights of the federal government to use it as described in their funding agreement.

V. The parties shall separately agree to more specific details regarding data elements to be used in the development of data systems models, which data elements can be confidentially and securely shared by [AGENCY 1] and [AGENCY 2] , and for any other data agreed upon by the parties, and the types of confidentiality restrictions that will apply to each.

VI. All data and information about the systems being developed will be kept confidential for five (5) years after termination of this agreement. The parties shall not disclose such Confidential Information except to each other. If such Confidential Information is disclosed to any party to this agreement or to its subcontractor, the party disclosing the information will assure that such disclosure shall be in writing and marked as Confidential Information. The parties agree to use such Confidential Information only for the purposes of this Agreement. The parties agree shall assure that its subcontractor agrees to keep all such Confidential Information confidential for five (5) years after the termination of this Agreement; provided that the receiving Party's obligations hereunder shall not apply to information that: (i) is or later becomes part of the public domain through no fault of the receiving Party; or, (ii) is received from a third party with no duty of confidentiality to the disclosing party; or, (iii) was developed independently by the receiving party prior to disclosure; or, (iv) is required to be disclosed by law or regulation. Any information that is transmitted orally or visually, in order to be protected hereunder, shall be identified as such by the disclosing party at the time of disclosure, and identified in writing to the receiving party, as Confidential Information as defined in this paragraph, within thirty (30) days after such oral or visual disclosure.

Figure 11-2. A Sample Memorandum of Understanding.

VII. No data as described in paragraph II will be shared with a party outside this agreement without the expressed consent of the party providing the data. At the end of five (5) years after execution of this agreement, or the cancellation of this MOU, whichever comes sooner, such data will be provided back to the data originators and destroyed by other partners, unless the other partners are authorized in writing by the data originators to maintain the data.

VIII. For the purposes of scientific publication and public release of detailed data, maps, and analyses, each MOU partner shall retain ownership and control of data it originated, and the data may not be provided by the other parties to any other agencies or individuals or utilized for analyses without the originator's consent. All parties to this MOU shall jointly own data analyses generated jointly under this MOU. No party shall publish or release the joint analyses conducted under this MOU without the review and approval of the other parties, unless otherwise required by law. Public posting of this information may be considered, depending on its usefulness and interest to the public and pending approval from the originating state. Press releases and press contacts shall be coordinated among the public affairs groups of each party.

IX. All project personnel, whether or not employed, who receive systems data and information for use in this project shall sign individual Non-Disclosure Agreements.

X. This agreement may only be amended in a writing signed by all parties.

XI. This agreement shall be effective upon execution by all parties and shall remain effective until such time as it is cancelled by thirty days written notification by any of the parties to each of the others.

IN WITNESS WHEREOF, this Memorandum of Understanding has been duly executed by the parties hereto on the day and year appearing following their respective signatures.

[AGENCY 1]
By: _____
Title:
Dated: _____/_____/_____

[AGENCY 2]
By: _____
Title:
Dated: _____/_____/_____

It appears as though the size of the jurisdiction is proportional to the level of bureaucracy required. Our experience in developing an agreement between agencies in Arizona and agencies in California follows this premise.

Negotiating a contract between the University of Arizona and ARJIS (Automated Regional Justice Information System) of Southern California required six to nine months of discussion between legal staff, contract specialists, and agency officials. We are hopeful that many of the solutions to barriers in that process may be applied to the formation of formal agreements for information sharing with other agencies across state boundaries.

TPD has recently developed a generic Inter-Governmental Agreement (IGA) that could be adopted between different law enforcement agencies. This IGA was condensed from MOUs (Memorandum of Understanding), policies, and agreements that previously existed in various forms between numerous agencies. The IGA was drafted in a generic manner, including language from those laws, but excluding reference to any particular chapter or section. This allowed the required verbiage to exist in the document without being specific to any jurisdiction.

Sharing of information between agencies with disparate information systems has also led to bridging boundaries between software vendors and agencies (their customers). We took care not to violate licensing terms by insuring that non-disclosure agreements existed and that contract language assured compliance with the vendors' licensing policies.

We believe MOUs and IGAs can be used as templates of information sharing agreements and contracts, and can serve as a component of an ISI partnership framework. A sample MOU template is shown in Figure 11-2. Institutions and agencies are encouraged to freely adopt and modify this template for their purposes.

11.4 The COPLINK Chronicle

We include below a chronicle of funding, research and development, and media reports of relevance to our COPLINK project. Many agencies, partners, and individuals have contributed significantly to the success of this program, which has grown from its humble academic research roots to wide-spread deployment and impact in public safety and homeland security.

The COPLINK system, which has been cited as a national model for public safety information sharing and analysis, has been adopted in more than 100 law enforcement and intelligence agencies. The COPLINK research had been featured in the *New York Times, Newsweek, Los Angeles Times, Washington Post,* and *Boston Globe,* among others. The COPLINK project was selected as a finalist in 2003 for the prestigious International

Association of Chiefs of Police (IACP)/Motorola 2003 Webber Seavey Award for Quality in Law Enforcement. COPLINK research has recently been expanded to border protection (BorderSafe), disease and bioagent surveillance (BioPortal), and terrorism informatics research (Dark Web), funded by the NSF, CIA, and DHS.

- September 1994-August 1998, NSF/ARPA/NASA, Digital Library Initiative (DLI) funding: Selected concept association and data mining techniques developed under the DLI program.
- July 1997-January 2000, DOJ, National Institute of Justice (NIJ) funding: Initial COPLINK research -- database integration and access for a law enforcement Intranet.
- January 2000, first COPLINK prototype: Developed and tested in the Tucson Police Department.
- May 2000, Knowledge Computing Corporation (KCC) founded: KCC received venture capital funding and licensed COPLINK technology.
- January 7, 2001, Arizona Daily Star: "Technology developed in Tucson is helping police catch criminals faster. COPLINK products let police agencies rapidly share crime information across jurisdictional line."
- July 2001, POLICE magazine: "COPLINK shifts and shares information – fast."
- October 23, 2002, Tucson Citizen: "Tucson cops, local software to help in D.C. sniper probe."
- November 2, 2002, New York Times: "An electronic cop that plays hunches." COPLINK was used to assist in the Washington, D.C. sniper investigation.
- November 7, 2002, Washington Post: "A missing link most wanted."
- November 18, 2002, Life Week magazine (Chinese): "A Sherlock Holmes for the Internet age."
- January, 2003, Public Technology: "COPLINK project receives the PTI Technology Award."
- March 3, 2003, Newsweek magazine: "A Google for cops."
- April 15, 2003, ABC News: "Google for cops."
- July 17, 2003, Boston Globe: "Software helps police draw crime links."
- August 19, 2003, Dodge City Daily Globe: "Northwest Kansas law enforcement to use program to sift through records."

- December 3, 2003, Motorola.com: "Tucson Police Department's COPLINK project was named a finalist of the prestigious Webber Seavey Award for quality in law enforcement."
- December 6, 2003, Los Angeles Daily News: "Cops can hit the links soon. New search engine would catalog, interpret data for investigations."
- September 2003-August 2005, NSF, DHS, CNRI funding for BorderSafe project: Cross-jurisdictional information sharing and criminal network analysis.
- September 2003-August 2006, NSF, Digital Government Program funding for Dark Web project: Social network analysis and identity deception detection for law enforcement and homeland security.
- August 2004-July 2008, NSF, Information Technology Research (ITR) Program funding for BioPortal: A national center of excellence for infectious disease informatics.

11.5 Future Directions

Forming a sustainable, win-win collaboration partnership between academics and selected law enforcement or intelligence agencies is difficult and, yet, potentially fruitful. In our COPLINK experience, we have seen that such a collaboration bears fruits in scientific innovation and social impact. We believe that we have made significant contributions to information sharing, crime data mining, deception detection, criminal network analysis, and disease surveillance research. We have also witnessed, first-hand, criminals arrested and lives saved as a result of public safety agencies using our technologies.

In the next decade, we envision significant breakthroughs in several areas. The BorderSafe project will continue to contribute to border safety and cross-jurisdictional criminal network analysis research. The Dark Web project will help create an invaluable terrorism research testbed and develop advanced terrorism analysis methods. The BioPortal project will contribute to the development of a national or even international infectious disease and bioagent information sharing and analysis system.

11.6 Questions for Discussion

1. How can you identify law enforcement and security agencies in your neighborhood or city that are interested in collaborating with you?
2. What are some ways to create a research lab that can handle potentially sensitive and confidential information? What are the roles and obligations of research scientists and students?
3. How do you work with university contracting and legal offices to develop the memorandum, license, and agreement for partnering agencies?
4. What are some ways to deliver immediate values to the partnering agencies during a research process?