

**Global Justice Information Sharing Initiative (Global)
Global Privacy and Information Quality Working Group (GPIQWG) Meeting**

Washington, DC
November 17–18, 2010

November 17, 2010—Meeting Summary

Background and Purpose

The U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), and the Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group (GPIQWG) convened a meeting on November 17, 2010, in Washington, DC, at 8:30 a.m. The Honorable Anthony Capizzi (Judge Capizzi), Montgomery County, Ohio, Juvenile Court and GPIQWG Chair, led the meeting in furtherance of and alignment with the GPIQWG's *Vision and Mission Statements*.

The following individuals were in attendance.

Chair

The Honorable Anthony Capizzi

*Montgomery County, Ohio, Juvenile Court National
Council of Juvenile and Family Court Judges*

Vice Chair

Mr. Phil Stevenson

Arizona Criminal Justice Commission

Devon B. Adams

*Criminal Justice Data Improvement Programs
Bureau of Justice Statistics
U.S. Department of Justice*

Owen Greenspan

*SEARCH, The National Consortium for Justice
Information and Statistics*

Jennifer Alkire

*Biometric Center of Excellence
Criminal Justice Information Services Division
Federal Bureau of Investigation*

Bob Greeves

*Office of Justice Programs
U.S. Department of Justice*

Robert Boehmer, GAC Chair

National Criminal Justice Association

Barbara Hurst, Esquire

Rhode Island Office of the Public Defender

Alan Carlson, Esquire

Superior Court of California, County of Orange

Erin Kenneally, Esquire

eLCHEMY, Incorporated

Michael Chamberlain

California Department of Justice

Nancy Kolb

*Center for Social Media
International Association of Chiefs of Police*

Colonel Steven Cumoletti (GAC member)

*Deputy Superintendent
New York State Police*

Michael McDonald

Delaware State Police

Lieutenant Kathleen deGrasse

Illinois State Police

Sheriff Michael Milstead

Minnehaha County Sheriff's Office

Becki Goggins

*Alabama Criminal Justice Information Center
& CONNECT*

Joe Mollner

Boys and Girls Clubs of America

Lieutenant Leo Norton

Los Angeles County Sheriff's Department

Dave Russell
NOVARIS

Steve Schuetz (proxy for Bill Ford)
National Institute of Justice

Steve Serrao
Privacy and Security Committee
IJIS Institute

Steve Siegel
Denver District Attorney's Office

Tammy Woodhams
National Criminal Justice Association

IIR Staff
Christina Abernathy
Institute for Intergovernmental Research

Terri Pate
Institute for Intergovernmental Research

Welcoming Remarks and Introductions

Chairman Capizzi welcomed everyone to the November 17–18, 2010, GPIQWG meeting. Introductions were made around the room. He informed the group of the Global Advisory Committee's (GAC) approval of the biometrics primer, titled *Privacy and Information Quality Risks: Justice Agency Use of Biometrics*, and the IQ Series Overview, titled *Information Quality Series Improves the Quality of Justice Information*. Following this, he provided an update on the Global Standard Package task team and introduced the GPIQWG Product Development Strategy (a one-page handout illustrating GPIQWG's routine method for product development). He presented the meeting summary and asked for approval.

Chairman Capizzi reviewed the agenda with the group and pointed out that the first day's focus would be on full-group discussion and presentations, followed the second day by breakout task teams. He announced the next meeting, which will be on February 23–24, 2010, in Nashville, Tennessee.

Global Updates

GAC Chairman Robert Boehmer provided a GAC and Global Executive Steering Committee (GESC) status update. Bob referred the group to the Global Highlights newsletter included in the meeting materials. The Global charter was renewed by the Attorney General (AG). He stated that pending legislation would give more permanency to Global, though it may take several years to be passed by the U.S. Congress. For now, the AG has renewed our charter for another two years.

Global approved many products, such as the renamed "*Global*" *Justice Reference Architecture* (which builds on products developed by the working groups, including privacy products). We are bringing in other providers that touch the justice system, such as health providers, etc. Ms. Woodhams raised the issue that there are a number of different products, such as from IJIS Institute and others, where JRA is referenced. With the name change to Global JRA rather than JRA, how does the GAC want us to reference this? Chairman Boehmer stated that the Global Outreach Working Group (GOWG) would be addressing this at its next meeting.

At the GAC meeting, there were new attendees from Fire and Emergency Medical Services (EMS), and the GAC is considering how to better collaborate with them. Chairman Boehmer stated that the GAC recommended the line officer video (roll call) for use in broader audiences (e.g., corrections, probation and parole). It was also suggested that the current video be field-tested to these broader areas. Chairman Boehmer indicated that if slight tailoring to the video was feasible, the GAC would definitely explore this retrofit with the Institute for Intergovernmental Research (IIR).

Chairman Boehmer noted that the relationship between Global and BJA began ten years ago and that a ceremony was held to celebrate the ten-year anniversary and to acknowledge Global's accomplishments and goals for the future. He complimented IIR and IIR staff for their hard work and mentioned that the ceremony included this acknowledgement.

He reminded the group of the next GAC and Global Executive Steering Committee (GESC) meetings: GESC, April 19, 2011, and GAC, April 20, 2011. He talked about the State of Global meeting held on November 16, 2010, and

the group's work on outlining a report to the AG. The primary focus of this report, from the perspective of a Federal Advisory Committee, is where we plan to go and our advice to the AG.

A new topic to be discussed later today (as tasked by the GAC) is social networking in the investigative arena and the privacy implications of that activity. Another topic the GAC is looking at is cloud computing (e.g., Google and Google documents; e-mail is retained on the Internet with attachments on a server), which is a new trend, but there are associated privacy and technical issues. Cloud computing stores the files and products from your server onto a Web-based server. This reduces costs and hardware and makes work more efficient. Right now, we are getting a briefing paper from another group, but this may come back to GPIQWG to address the privacy issues. The Global Security Working Group and the Global Infrastructure/Standards Working Group will both have components of this project.

Chairman Boehmer referred the group to the executive summaries for the other Global Working Groups, which were contained in the meeting materials. As you take a look at their goals and products, you may want to keep in mind how those may affect our group and touch on privacy and information quality issues.

The GESC/GAC Experience

GPIQWG Vice Chair Phil Stevenson, Arizona Criminal Justice Commission (ACJC), attended the fall GAC/GESC meetings for the first time. He wanted to share with the group his perspective on how this advisory body completes its work and how products are presented/reviewed/approved. He noted that there was virtually no discussion on the GPIQWG products put forth for approval, allegedly because of the good work, but that emphasized [to him] our responsibility to critically address these issues fully prior to product submission. GPIQWG is at the forefront of many issues, and the time we spend in discussion, draft work, revisions, and testing is well-noted by GAC members when they review our products. Ms. Barbara Hurst noted some concern about the lack of discussion because there was potentially less ownership. Chairman Boehmer stated that this is an issue that they struggle with but that GAC members trust the working group product development processes. He agreed that soliciting involvement by the GAC is a continually evolving process.

Mr. Stevenson stated that the GAC is a unique collaboration among local, state, tribal, and federal partners. Through GPIQWG and the GAC members, constituents can bring their issues forward. Two years ago, Mr. James Patrick McCreary, BJA, compared the GAC to a wheel and GPIQWG to one of the hubs of the wheel. It was even more apparent that this is true when the GAC/GESC was observed in action. The work and efforts of GPIQWG affect the other working groups. Seeing the process helped clarify GPIQWG's role and connection to the other working groups. Finally, the GAC membership's broad representation is quite impressive. Federal agency directors are in attendance, which is an uncommon audience in most situations. All members participate actively. It is a level of collaboration that Mr. Stevenson has not seen in other arenas, which speaks to the thoughtfulness with which this initiative was structured. He encouraged GPIQWG members to attend future GAC/GESC meetings.

Chairman Capizzi noted that the GAC meetings are similar to congressional hearings because of their formality. There may be 100 GAC members around the table, but there are more than 300 agency representatives in the audience. It is a unique event in which you have access to the many influential leaders from the justice community, and they listen. The federal directors respect the work that is being done.

Corrections and Community Service Provider Information Sharing: Privacy Issues

Mr. Bob Greeves, Office of Justice Programs (OJP), DOJ, provided an overview to the group regarding the confidentiality of patient records and alcohol and drug abuse patient records in the offender intake and reentry area. Penalties associated with violation of 42 U.S.C. §§ 290dd-3 and 290ee-3 Confidentiality of Patient Records, and violation of 42 CFR Part 2, et seq. Confidentiality of Alcohol and Drug Abuse Patient Records, are negatively affecting the timely sharing of assessment and treatment information for arrested and/or convicted offenders with alcohol or drug abuse issues who are entering, leaving, or transferring within the criminal justice system (including postrelease supervision and revocation from probation/parole to a correctional facility). This presents a public safety issue in cases where offenders reentering the community may not receive timely substance abuse treatment to reduce the likelihood of failure. In addition, it can result in the inefficient and/or duplicative expenditure of public funds in a time of financial crisis in states and municipalities and failure to provide needed service to offenders who may need immediate help during or immediately after intake into a correctional facility. It is not just about dealing with drug abuse but also mental health and other health-related services.

Three pilot sites are taking place on this issue, but, in all cases, they are facing roadblocks in their ability to resolve all information sharing issues because of the health information privacy legal concerns. All are trying to deal with these cases using the consent to release, but they are still struggling. Though the pilot site meetings are bringing people together who previously were not talking to each other, in nearly every case the attendees are finding that they cannot share because of the legal restrictions (cited above).

There are two recommendations: To advise the AG of this issue and suggest discussion with the Health and Human Services (HHS) folks and for GPIQWG to look at this issue.

There is a lack of information from the community to corrections intake, during transfer, and release back into the community. Information sharing, regulations in some cases, and personal interpretations of the regulations contribute to this problem. Agencies that provide services (e.g., substance abuse) sharing information with the courts represent an even more difficult issue. Chairman Capizzi stated that this is also an issue with the drug court and juvenile court he presides over. Discussion ensued regarding medical information and the priority being custodial versus not “for the good of the people.” A particular piece regarding reentry and public safety is with regard to sex offenders and where those treatments are with regard to public safety versus medical record privacy. This also exists in other arenas, such as victims and domestic violence. We have acknowledged that an interagency agreement between agencies is the best way to protect them.

CONNECT Project—A Model of Global Implementation

Ms. Becki Goggins, Alabama Criminal Justice Information Center and CONNECT, provided a presentation on the CONNECT project. CONNECT is a consortium of participating states—Alabama, Wyoming, Nebraska, and Kansas. The Web site is connectconsortium.org. The project currently focuses on the sharing of one data set—drives license information. The states in the project were chosen because all have robust justice information systems. CONNECT’s vision is for criminal justice personnel to have simple, secure, and cost-effective access to rich interstate information to help states prevent and effectively respond to crime. CONNECT benefits include more users, more data, and more affordability (especially for smaller agencies that cannot afford T1 connections into the Nation Crime Information Center [NCIC], Nlets, vendor records management systems [RMS], etc.). For the proof of concept, they started by sharing driver’s license information. CONNECT uses the Global Federated Identity Privilege Management (GFIPM), defining two data sets, and the National Information Exchange Model (NIEM) Information Exchange Package Documentation (IEPD), Global Justice Reference Architecture (GJRA) Web Services, and the GPIQWG *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* (Privacy Guide). A lot of the issues we needed to resolve were solved by Global products. NIEM provided the semantic precision so each agency and agency type used the same vocabulary. Each participating agency had different architectures and technologies. The JRA was used to allow each agency to retain its architecture. Credentialed role-based level of access, using GFIPM, was developed.

The CONNECT project addressed privacy head-on, using Global’s *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives*, and performed PIAs for all four states prior to privacy policy development. Alabama now has a PIA on every data store accessed and has updated its privacy policy as a result of those PIAs. Each state looked at its legal requirements, which was somewhat of a challenge. Policies were needed for secondary dissemination, logging and auditing requirements had to be addressed, and enforcement procedures for misuse had to be worked out with all four. CONNECT had to decide how we were going to respond, across states, for abuse. Each piece of data is retained within the owning state; CONNECT does not store data. As such, each owning state is responsible for the quality of its information.

GFIPM resolved the issue of having to use different access and passwords for each database. User management was distributed to the state level. This mechanism defined how to set up identity providers and clarify role-based access. Further, through the technological solutions, CONNECT pursued the assurance of privacy protections in place to support the privacy policy.

One problem the consortium had to deal with was cross-jurisdictional auditing and enforcement. CONNECT developed a public Web site to provide the privacy policy and information on the project. Kansas and Alabama have ratified their privacy policies, and currently Nebraska and Wyoming are working to ratify theirs. Until all policies are adopted, the program will not officially be turned on in production scale.

CONNECT’s mission in adopting all of these standards was to make it easier, once other states do the same, to share information. The plan is to later add more data such as that from corrections and the courts, as well as crash data, citations, pardon/parole information, domestic violence reports, protection orders, vehicle information, etc. CONNECT is working to help more users finalize these service specifications.

Justice Use of Social Networking Sites—Privacy Implications

Chairman Boehmer and Ms. Nancy Kolb, International Association of Chiefs of Police, Community Safety Initiatives and the IACP Center for Social Media, discussed the privacy implications of justice agency use of social networking sites. Ms. Kolb stated that the new IACP Center for Social Media is performing research on what use of social networking sites is taking place (in law enforcement), the trends and key issues, and trying to determine what the field may need. Overwhelmingly, agencies have stated that they need a policy for this use. There are dozens of cases of misuse that are seen in the media. The IACP has worked to develop a model privacy policy. The policy addresses both official use of social networking sites (e.g., for investigative purposes) and officers' personal use. Facebook pages are considered a public record. Boca Raton, Florida, has posted a notice on its Facebook page that if you become a friend, it may become a public record. In September 2010, the IACP did a survey of IACP members to determine use, barriers, etc. IACP received 783 responses from law enforcement agencies. The vast majority (56 percent) were using it for investigations (Facebook, MySpace, Twitter, YouTube, etc.). While networking sites are a great resource for law enforcement, we need to provide education on appropriate use. About 40 percent of the respondents said they were using it for community outreach and 37 percent said they were using it for background investigations for law enforcement personnel. Agencies that had said they were not using it were asked whether they were considering future use. Most said they were considering it within the following six months. These agencies were asked what their barriers had been, and most said cost, time and resources, privacy issues, etc. The center provides online information on the top 20 social media sites with information on law enforcement use and tips for appropriate usage and other helpful tools.

On the IACP Center for Social Media Web site, socialmedia@theiacp.org, a series of fact sheets is provided on the different platforms and uses (from recruiting, to preventing crime); topic-focused resources (e.g., malicious use of social media, privacy); a directory of law enforcement agencies using social media, including background and demographic information; as well as links to the center's specific social media page. This allows agencies that are not using social media to see what other agencies, similar in size, are doing. A blog is also available to provide field experience. This issue is so new that the case law on what you can/cannot do is not yet consistent.

BJA is looking at developing a fact sheet on Facebook safety for officers (for example, undercover officer safety, departments posting photos of their group of officers as a public relations piece). BJA funded a grant to the IACP for the Center for the Prevention of Violence Against the Police, and this effort will fall under that initiative.

Law enforcement department pages have been found to be very positive. For example, the Virginia State Police started its own page, and it has close to 23,000 folks as friends now, many of whom have provided tips.

IACP is working on a related project in partnership with the U.S. Department of Defense regarding a set of guidelines for background investigations (to be released in December 2010) related to security clearances for law enforcement and military personnel. These guidelines describe how to use social media to vet applicants and get information to verify information they have provided. Also provided is guidance on access and password use and security.

At the last IACP conference, there were six different workshops on social media, all standing-room-only because of their popularity. We are building a two-to-four-hour curriculum on what chiefs need to know on social media.

Chairman Boehmer talked about his work on behalf of NCJA with the Office of Community Oriented Policing Service (COPS) on social networking for investigative purposes. Law enforcement has not been provided with a lot of guidance on usage of social media. NCJA/COPS surveyed prosecutors who indicated that they were not certain how judges were going to react to social media violation issues. The NCJA/COPS issue paper contained in the meeting materials was developed to provide a quick snapshot of the issues and to provide recommendations. Page 6 of the document, *Social Networking and Urban Violence Forum*, provides the list of recommendations regarding a guide, perhaps a quick-reference guide, for law enforcement.

Chairman Capizzi asked Mr. Boehmer what GAC envisions as GPIQWG's priority in this area. The direction is to determine what the landscape is, what work is already being done, and where GPIQWG can participate/collaborate or where there are gaps that may require resources and guidance, if any. Part of Global's task is to figure out what is out there. We do not know what is being done by courts, corrections, probation and parole, and other areas—not just law enforcement. Whatever we produce can be included on the IACP Web site.

Defining Privacy and Related Concepts

Ms. Barbara Hurst, Rhode Island Office of the Public Defender, reviewed the tasks assigned at the July 13–14, 2010, GPIWG meeting to revise the content of the guide and to postpone the discussion of “the definition of privacy” for the November 17–18, 2010, meeting. We have been discussing since December 2009 the issue of what constitutes a privacy issue. The task today is to address section four of the Privacy Guide, Understanding Privacy Concepts,. Today, we need to work out what constitutes a privacy issue and to review and clarify the recommended language in section four.

Ms. Abernathy provided an update on the tasks completed on the privacy guide revisions since the July meeting and referred the group to the *Catalog of Global Products Impacted* that illustrates a list of Global products that may need to be updated if we change the definition of “privacy.”

Ms. Hurst reviewed the revised structure of section four, “Privacy Overview” with the group and discussed recommended content for this chapter. The recommendations included a framework for decision-makers on how one determines “what is a privacy interest” and how an agency applies its privacy policy to those issues. The biometrics framework helped individuals think about recognizing privacy issues in a justice arena. Some of the recommended language explains what is meant by terms used in the rest of the policy, e.g., civil rights and civil liberties.

Regarding personally identifiable information, we needed to make it clear that we are talking about pieces of data that themselves may not identify a unique individual but are building blocks to identifying an individual.

Informational privacy is a First and Fourth Amendments issue, tied to specific and concrete spacial considerations and particular situations. For example, the negligent handling of data may not be considered a Fourth Amendment issue. The negligent handling of data, however, is a huge issue for us. Issues such as the interchange between public and privacy information, commercial private networks, and government use of those networks do not really fit under the Fourth Amendment.

Mr. Carlson stated that what we are doing is to state “in what context” are we referring to privacy: the kinds of privacy issues that are important enough that you have to have a privacy policy to cover them. What privacy issues does the privacy policy cover? We now know a lot more today than we did in the original drafting of the Privacy Guide. We need to state the situations and issues for which we are writing a policy for to help enable users of the Privacy Guide come to an understanding.

Furthering the GPIQWG Information Quality Series

Mr. Stevenson asked the group whether there should be more work completed on the GPIQWG Information Quality (IQ) Series. We need to do a better job of outreach and pushing these materials out to constituents. Do we need additional tools? It has been suggested that we pursue a state-level pilot of the IQ Self-Assessment Tool. Discussion ensued over whether GPIQWG needs to consider development of additional products at this time. The consensus was that the group did not need to develop new products.

Action Item: GPIQWG will task GOWG with reevaluating the outreach for this product: how to get local jurisdictions to embrace and use these tools.

GPIQWG 2011 Draft Business Plan

Judge Capizzi introduced the 2011 draft business plan to the group. He reviewed each section and deliverable with the attendees, including the membership list. He discussed the importance of attendance and having the right expertise at the table to achieve GPIQWG goals. He referenced the open seats (tribal, juvenile justice). Ms. Hurst raised the question of why we do not have a membership seat for a privacy, civil rights, and civil liberties professional. The group agreed that the addition of another funded membership seat would need to be approved by the GESC.

Action Item: Mr. Boehmer and Judge Capizzi will raise the issue of a creating a membership seat for a privacy, civil rights, and civil liberties professional (e.g., privacy advocate) at the January GESC meeting.

Judge Capizzi reviewed each proposed product for 2011. The group adjusted the language and proposed work as a result of several discussions today (e.g., social networking, piloting the IQ Self-Assessment Tool) and also identified deadlines for completing these projects.

Action Item: Per Mr. Greeves, OJP would like an indication of whether GPIQWG will want to weigh in on the issue of offender reentry. Judge Capizzi will raise this issue with the GESC at its January planning meeting.

Action Item: Cloud computing is suggested as an addition to the February agenda.

Next Steps and Closing Remarks

Judge Capizzi stated that tomorrow, the structure will be breakout format. He announced that instead of four task teams (based on the discussions on IQ Series and social networking today), there will only be two task teams: The Denver Case Study Task Team and the Privacy Task Team. He reviewed the goals of the task teams and thanked everyone for their participation.

The meeting was adjourned at 4:30 p.m. EST.

**Global Justice Information Sharing Initiative (Global)
Global Privacy and Information Quality Working Group (GPIQWG) Meeting**

Washington, DC
November 17–18, 2010

November 18, 2010—Meeting Summary

The GPIQWG meeting was reconvened at 8:30 a.m. EST on Thursday, November 18, 2010. The following individuals were in attendance.

Chair

The Honorable Anthony Capizzi

*Montgomery County, Ohio, Juvenile Court National
Council of Juvenile and Family Court Judges*

Vice Chair

Mr. Phil Stevenson

Arizona Criminal Justice Commission

Devon B. Adams

*Criminal Justice Data Improvement Programs
Bureau of Justice Statistics
U.S. Department of Justice*

Jennifer Alkire

*Biometric Center of Excellence
Criminal Justice Information Services Division
Federal Bureau of Investigation*

Robert Boehmer, GAC Chair

National Criminal Justice Association

Alan Carlson, Esquire

Superior Court of California, County of Orange

Michael Chamberlain

California Department of Justice

Ayn H. Crawley

*Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security*

Colonel Steven Cumoletti (GAC member)

*Deputy Superintendent
New York State Police*

Becki Goggins

*Alabama Criminal Justice Information Center
& CONNECT*

Owen Greenspan

*SEARCH, The National Consortium for Justice
Information and Statistics*

Bob Greeves

*Office of Justice Programs
U.S. Department of Justice*

Barbara Hurst, Esquire

Rhode Island Office of the Public Defender

Erin Kenneally, Esquire

eLCHEMY, Incorporated

Jennifer Luttmann

*Combined DNA Index System (CODIS)
Federal Bureau of Investigation*

Michael McDonald

Delaware State Police

Sheriff Michael Milstead

Minnehaha County Sheriff's Office

Joe Mollner

Boys and Girls Clubs of America

Lieutenant Leo Norton

Los Angeles County Sheriff's Department

Dave Russell

NOVARIS

Steve Schuetz (proxy for Bill Ford)

National Institute of Justice

Steve Serrao

*Privacy and Security Committee
IJIS Institute*

Steve Siegel

Denver District Attorney's Office

Carl A. Wicklund, GAC Vice Chair

American Probation and Parole Association

Ms. Tammy Woodhams
National Criminal Justice Association

IIR Staff
Christina Abernathy
Institute for Intergovernmental Research

Terri Pate
Institute for Intergovernmental Research

Judge Capizzi welcomed everyone and introduced guest observer Ms. Jennifer Luttmann, Combined DNA Index System (CODIS), Federal Bureau of Investigation. He asked for questions from yesterday's discussion. Mr. Stevenson voiced his support for the reentry issue presented by Mr. Greeves. Judge Capizzi indicated that the group will follow up with future agenda topics to further the discussion prior to deciding whether it is a priority for the group.

Today's work will focus on two task teams: (1) The Privacy Task Team, which will work on the revisions to the Privacy Guide, particularly, section four (Privacy Overview), and (2) the Denver Case Study Task Team, which will identify the privacy issues associated with familial DNA searching, in preparation for drafting the privacy policy for Denver.

DHS Office of Civil Rights and Civil Liberties

Ms. Ayn Crawley, Office of Civil Rights and Civil Liberties, U.S. Department of Homeland Security (DHS), provided a brief overview of her department's efforts to train state and local fusion centers, both in on-site and train-the-trainer programs. To date, the department has trained 66 of the 72 fusion center officers. It also provides a Web site with training materials.

Another goal for this effort is to strengthen the privacy and civil liberties officer network. We found that, of the 66 people mentioned earlier who attended training, a third (22 to be exact) had only recently been appointed as fusion center privacy officers. A trend DHS has observed is that some centers rotate positions. Ms. Crawley stated that they have tried to educate center directors that this is an ongoing position and that selecting an individual with the right skill set and training is important.

Mr. Wicklund asked whether DHS tests attendees after the training. Ms. Crawley stated that the department has not done so yet but that one of the goals is to implement posttraining testing.

Breakout Sessions

Judge Capizzi adjourned the meeting into breakout sessions. The following is a list of attendees per task team. The two teams met from 9:00 am until 11:30 a.m. EST. Chairman Capizzi floated between both task teams.

Privacy Task Team

1. Team Lead: Barbara Hurst
2. Ayn Crawley
3. Steven Cumoletti
4. Bob Greeves
5. Erin Kenneally
6. Mike McDonald
7. Mike Milstead
8. Joe Mollner
9. Terri Pate
10. Steve Serrao
11. Steve Schuetz
12. Carl Wicklund
13. Tammy Woodhams

Denver Case Study Task Team

1. Team Lead: Steve Siegel
2. Christina Abernathy
3. Devon Adams
4. Jennifer Alkire

5. Bob Boehmer
6. Alan Carlson
7. Michael Chamberlain
8. Becki Goggins
9. Owen Greenspan
10. Jennifer Luttmann
11. Leo Norton
12. Dave Russell
13. Phil Stevenson

GPIQWG Task Team Status Reports

Chairman Capizzi requested that each task team lead provide status reports on its work and discussions. Below are synopses of these status reports.

Privacy Task Team

Ms. Hurst, who led the Privacy Task Team, stated that the group focused both on section four (“Privacy Overview”) of the Privacy Guide and the universal concepts portrayed in the Guide. One issue the team discussed was the dissemination of information within the criminal justice community. What happens to information when it leaves this community, and what privacy issues are implied? The following are highlights from the task team discussions:

- What are privacy and civil liberties? First, what is privacy, and then, what are informational privacy and civil liberties? Finally, what are the privacy concerns for the sharing of information?
- To apply the privacy principles in the Privacy Guide to the sharing of information, we have to understand and help the readers understand what privacy is—it is the objectives of chapter 4, “Foundational Concepts.” We must provide a clear understanding of privacy and privacy-related concepts.
- Chapter 4 was renamed “Understanding Foundational Concepts.”
- The introductory paragraph should describe what you are about to read and should include the goals of the chapter.
- Section 4.1.1 states explicitly that we are not dealing with privacy concerns—rather privacy interests versus privacy rights. For example, victim information is public in many places. There is a privacy interest in not sharing the victim’s name and address in the documents that get shared within the justice system, but there is no privacy right being asserted. Crime mapping of domestic violence and sexual assault victims is the issue. The justice argument is that people need to know where rapes are occurring.
- There should be a sentence about balancing individual interests against government purpose. Also an example about interagency sharing (e.g., fusion centers).
- The section on contextual privacy will be retained with the addition of a new bullet about criminal justice use of online social networking.
- Section 4.1.3 talks about public versus private information. There are three strains: (a) whether publicly developed information is presumptively public information; (b) whether dissemination by public agencies is more intrusive than that by private entities; and (c) whether individuals or entities fulfilling public roles have different or fewer protected privacy interests than do private individuals. Suggest placing (c) in a footnote.
- Section 4.3 should be renumbered as 4.1.1. What is personally identifiable information (PII)? Not all PII is protected. Maybe this topic should go after contextual privacy in this section. While a name and address in the phone book is public information, if the same information is in connection with a pornography Web site, this implicates privacy interests. The notion of PII is changing as conceptions of privacy change because PII is no longer static, traditional, and explicit first-order information like a name and address. Given the online environment, the unit of risk is no longer a first-order identifier; rather, it is a mosaic of information that can be attached to, or linked to, commonly referenced personal identifiers. For example, “race” plus “Zip code” could be an identifier. With only three pieces of information, such as date of birth, Zip code, and gender, one could identify 60 percent of the population. Erin Kenneally will review the PII section and provide examples.
- We need to include a positive statement in the PII section about the exchange of PII being necessary for various actors, such as law enforcement, to do their jobs. Additionally, the section should explore the concept of “information that is needed” versus “information that is wanted.” Are there legitimate purposes where information is needed?

- For the civil liberties discussion, the DHS Office for Civil Rights and Civil Liberties (CRCL) will provide examples of things it has been working on. Also, Ayn Crawley and her team at CRCL will review the guide to (a) insert “civil liberties” throughout, where appropriate; and (b) revise the section titled “What are Civil Liberties?” The CRCL team will also add real-life examples.
- Per Mike McDonald, there needs to be some discussion on the restrictions that travel with information. For example, when law enforcement information gets sent to the court, do the submitting entity’s restrictions travel with the information? For example, the case of the *State of Delaware v. Gannett News*. We should include a paragraph at the end of section 4.1.1 that states because it is information sharing, the end recipient always needs to be a consideration.

Denver Case Study Task Team

Mr. Steve Siegel led the task team discussion. He noted that there is a reference in Denver’s current familial DNA policy that if a law enforcement officer wants to utilize the familial DNA search capability, he will have to complete training. The training materials were provided for the task team in the meeting folders. Mr. Siegel also referred the task team to the comparison that Denver did between its current policy and the draft *State, Local, and Tribal Privacy Policy Development Template*, as well as a two-page document covering a review of the template as it relates to this capability.

Mr. Siegel provided the group with a brief background on this effort. Denver has solved 77 assaults using the familial DNA method, as well as others as they relate to burglary and auto theft (which are often predicate crimes). One effort under way in the biometric vendor industry is a prototype program called Fast DNA (aka “black box”), which is several years away from being ready for broad use but returns results within hours. While this may not be part of Denver’s program, eventually it may affect the crime-scene environment.

Mr. Siegel stated that the purpose of today’s discussion is to identify the privacy issues associated with familial DNA searching. When a familial DNA search is run against a local, state, or federal (e.g., CODIS) database and the hit is strong enough to meet criteria for a familial hit, what exactly does that give you? The resulting hit is not the end of the investigation. The result is actually an investigative tool for doing even more traditional police work to determine whether you have the right suspect for the crime. Our effort is what are the privacy issues that arise when you do familial searching?

Note: There is a difference between a partial match (the result of normal routine searches) and a familial search, which is a deliberative search to look for relatives. There is significant research by scientists as to what mathematical algorithms must line up for the result to be considered a match. This research defines how many alleles (genetic markers) the target profile must share with the subject DNA.

The group held a brainstorming session and came up with the following issues, related to their experiences with DNA in the field. There are several points for consideration regarding this discussion and the identified issues:

1. Not all of these may be relevant as issues and not all may be used in GPIQWG’s paper “Privacy Issues Associated with Familial DNA Searching.”
2. These reflect the random ideas put forth during an open discussion, each of which requires further exploration and research.
3. Each issue in bold reflects what the group considers to be concerns associated with this capability. Supporting information is provided to clear up or debate this concern.
4. It is important to note that the team will need to discern between issues related to DNA databases and issues related to familial DNA searching. Some of the issues cited below relate to DNA databases, alone.
5. Finally, the team needs to scope this effort. Is this an issue paper for agencies considering familial DNA searching or an issue paper to allay public fears? What exactly is the focus, and who is the target audience?

Issues Cited

- **Issue 1—Familial DNA Searching Will Result in Racial Profiling:** In fact, race is actually not known in this particular search. When a familial search is performed, the result is a top tier of, for example, 150 candidates that could be related using 15 discriminating alleles specific to identification (of which race is not included). Then, a search is performed on the Y chromosome to determine patrilineal heritage. If one male has the same Y type as the perpetrator, the next step is to look at birth records, criminal history records, etc., that would disprove the resulting match. In addition, CODIS also only stores these particular 15 alleles in its database, not the whole DNA typing; as such, race is not an indicator for CODIS either. What is released to law enforcement as a result of a familial DNA search is not the entire DNA profile; as such, race is not a factor.

- **Issue 2—Retention:** DNA samples have been collected legally since 1984. Though Denver does retain the original sample, for familial DNA search purposes, it only uses the 15 alleles referred to in Issue 1. Currently, in the United States there is no statute on DNA retention periods, though in Denver there are established expungement procedures for arrestees who are later exonerated and also destruction procedures for samples taken from individuals simply for the purpose of ruling them out in a crime scene investigation. However, retention of DNA samples from arrestees and unknown samples from crime scenes, does not invoke the Fourth Amendment.
- **Issue 3—Secondary Use (a Use for Which the DNA Was Not Originally Collected):** State and federal laws are exceptionally strict on the use of DNA only for (acknowledged law enforcement purposes) criminal identification and for missing persons. Federal citation—42 U.S.C. § 14132.
- **Issue 4—Who Is in the Database?:** There is a fear that not only criminals are in a DNA database. The FBI (re: CODIS) is very strict on who DNA is collected from. Per Ms. Luttmann, every state has different laws. Currently, approximately 25 states have recently passed legislation allowing the collection of DNA on all arrestees. While state laws allow states to determine what samples can be retained, national rules must be satisfied before states are allowed to submit the information to the national system (e.g., CODIS). Through the Justice for All Act, DNA is allowed to be placed in CODIS. Federal law allows DNA to be collected on non-U.S. citizens detained and anyone who is convicted of a felony crime. Also, every state is required to have an expungement process for convicted offenders and arrestees. Though non-U.S. citizens may not be required to be expunged at the state level, but they are required to be expunged at the national level.
- **Issue 5—What Happens to DNA Between Arrest and Conviction?:** In some states, the laws differ, but generally DNA is allowed to be collected upon a suspect's arrest and kept until the suspect is charged. Denver provides training and guidance to law enforcement with respect to how the familial DNA lead is used and perceived, with training on the sensitive handling of the information. [This issue requires more discussion.]
- **Issue 6—Scope of Consent (Prior Consent):** [This issue requires more discussion.]
- **Issue 7—Can Courts Compel a DNA Sample From a Sibling Who is Not in the Database?:** In the BTK case, a pathology sample was taken from the daughter without her consent. A DNA analysis was performed and her DNA compared with the suspect DNA, but this is different (a one-on-one case) than comparing a DNA sample against a whole database. Did the daughter have a legitimate expectation of privacy? Is it enforceable? There was no harm to her or liberty interests. However, privacy issues may be an issue if an individual provides a sample to his or her doctor for purposes of medical testing, unaware that it may be compelled later for other reasons.
- **Issue 8—Is a Familial DNA Lead Alone Probable Cause? Is It Enough to Go to a Judge and Get a Warrant?:** [This issue requires more discussion.]
- **Issue 9—Can An Arrest Be Made Solely on the Results of a Familial Lead?:** In fact, the answer is “No.” Other factors are considered, in addition to a familial DNA lead, such as geographic area, demographics, etc. In Denver, all other exhaustive leads have to have been investigated first before a familial DNA search can be performed. Other information also considered includes the suspect's prior arrests, for example. All investigative leads must be exhausted prior to a familial DNA search, and then, even with a familial lead, even more traditional police work must be performed with this lead to determine whether the right suspect has been arrested for the crime.
- **Issue 10—Is Familial DNA Searching Performed on Any Crime That Is Unsolved or Only Those That Pose a Particular Danger to Society?** The Fourth Amendment evaluates the “state's interest versus the violation of privacy rights.” For example, investigating a serial killer versus a car thief. [This issue requires more discussion.]
- **Issue 11—Are Routine Processes Ever Subverted?** In other words, are processes short-circuited in particular cases? For example, in certain urgent cases, such as one involving an active serial killer. [This issue requires more discussion.]
- **Issue 12—What Is the Decision to Perform a Familial DNA Search Based On?** Is there a formal process? First and foremost, each state must have the authority, whether by state statute, mandate, etc., to perform a familial DNA search. In Denver's case, in addition to authority, all leads must be exhausted before a request can be made through formal procedures for a familial DNA search. The request is formally reviewed prior to determining whether to do the familial DNA search.

- **Issue 13—If My DNA Is in the DNA Database, Does That Mean I Am a Suspect?:** DNA records are clearly marked if individuals have been excluded as suspects or if they are minors. Other factors are noted, such as if the perpetrator is male and the DNA result is female. [How does this translate to familial DNA searching?]
- **Issue 14—If My DNA Comes Up as a Potential Familial Lead, Am I a Suspect?:** No. The result would indicate that an individual may be related to the suspect; however, a ruling-out process that considers other factors is first performed. The goal is to narrow down the results to as accurate a match as possible.
- **Issue 15—What Is the Chain of Custody for Notification of the Lead? Can Anyone Receive That?:** The Denver policy states that the case report must be mailed or hand-delivered; chain of custody is reason for this. You want to limit to hard-copy case files. What is the electronic process?

Other discussion points:

- There are parallels between DNA and original fingerprint processing. For familial searches, when does the lab technician say that law enforcement should probably take a look at this individual? In the fingerprint world, the match may be close but not enough for an identification. DNA has more quantifiable reasons to give the information as a lead to the detective. The lab should adopt procedures that are carefully calibrated to provide investigatory leads of the highest quality—not to cast too wide a net. Scientific confidence based on mathematical statistics (probability).
- Does the lab make the determination to release the lead? What is the judgment call at the lab level to release? What are the practices for filtering prior to releasing the lead? In Denver, the lab comes up with the result, which then goes to a committee for review prior to release.
- Included in the Denver familial DNA search process is a family-tree analysis to determine who the family members are.
- When the lab releases the lead, is there follow-up to find out what happens? Is the investigative agency required to send results of the investigation back to the lab?
- There is qualifying language in the current Denver policy that the familial DNA searches are bound to unsolved cases. Should it be limited to that in the policy? Should the policy allow for the expanding technological abilities in which a familial DNA search may be performed in, for example, a misdemeanor case?
- Do identical twins have identical alleles? Yes.
- States have to make the decision to allow other states to search their databases. FBI's CODIS also guides this.
- Statistical thresholds for partial matches cannot be set exactly the same in each state because of the numbers in the database per state, which are different. There is a statistical calculation based on the size of the database. You have to make sure the threshold is appropriate based on the size of the database.

Next Steps and Closing Remarks

Chairman Capizzi stated that every presentation made yesterday prompted great discussion and debate. Today, during the task team discussions, everyone spoke up and had input, and he commended everyone for representing their constituencies in these efforts.

He asked if anyone had final points for discussions. Mr. Siegel informed the group that yesterday, November 17, 2010, the AG announced the Office of Tribal Justice as a separate component within DOJ.

Chairman Capizzi thanked everyone for their attendance and active participation at this meeting. He reminded them that the next meeting will be held on February 23–24, 2011, in Nashville, Tennessee.

The meeting was adjourned at 11:45 a.m.

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Wednesday, November 17, 2010

8:30 a.m. – 9:15 a.m.

Welcoming Remarks and Introductions

*The Honorable Anthony Capizzi, GPIQWG Chair and Judge,
Montgomery County, Ohio, Juvenile Court*

Topics

- ◆ Welcome new attendees (bios in meeting packets):
 - New Member: Ms. Jennifer F. Alkire, Management and Program Analyst, Biometric Center of Excellence, Criminal Justice Information Services Division, Federal Bureau of Investigation
 - Guest: Mr. Steve Serrao, Director, Memex LE Solutions, U.S., and retired Captain, New Jersey State Policy—representing the IJIS Institute
 - Guest: Ms. Becki Goggins, Division Manager, Uniform Crime Reporting Division Manager and Statistical Analysis Center Director, Alabama Criminal Justice Information Center and the CONNECT Program
 - Guest: Mr. Michael Chamberlain, Deputy Attorney General, Bureau of Forensic Services, California Department of Justice
 - Guest: Ms. Nancy Kolb, Senior Program Manager, International Association of Chiefs of Police, Community Safety Initiatives and the IACP Center for Social Media
- ◆ GAC-approved GPIQWG products:
 - Biometrics Primer—*Privacy and Information Quality Risks: Justice Agency Use of Biometrics*
 - IQ Series Overview—*Information Quality Series Improves the Quality of Justice Information*
- ◆ Global Standard Package meeting, October 28, 2010, Denver, Colorado
 - GPIQWG Product Development Strategy (overview in meeting packets)
- ◆ July 13–14, 2010, GPIQWG draft meeting summary
- ◆ Agenda overview
- ◆ Next GPIQWG meeting: February 23–24, 2010, Nashville, Tennessee

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Wednesday, November 17, 2010 (continued)

9:15 a.m. – 9:45 a.m.

Global Updates

Mr. Bob Boehmer, Global Advisory Committee (GAC) Chair and Director, American Institute for Public Safety Partnership, University of Illinois at Chicago, representing National Criminal Justice Association

Topics

- ◆ Upcoming GAC dates: GESG, April 19, 2010, and GAC, April 20, 2010
- ◆ October 2010 GAC meeting summary
 - Roundtable
 - 10-Year Anniversary Celebration
- ◆ Global Working Group updates

9:45 a.m. – 10:00 a.m.

The GESG/GAC Experience

Mr. Phil Stevenson, GPIQWG Vice Chair and Director, Statistical Analysis Center, Arizona Criminal Justice Commission

Topics

- ◆ GPIQWG product approval—the GAC process
- ◆ GESG meeting—steering the Global wheel
- ◆ GAC membership—broad representation

10:00 a.m. – 10:15 a.m.

Corrections and Community Service Provider Information Sharing: Privacy Issues

Mr. Bob Greeves, Policy Advisor, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice

Topics

- ◆ Issues at intake and reentry at pilot sites
- ◆ Maryland Department of Corrections issue paper

10:15 a.m. – 10:30 a.m.

Break

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Wednesday, November 17, 2010 (continued)

10:30 a.m. – 11:00 a.m.

CONNECT Project—A Model of Global Implementation

Ms. Becki Goggins, Uniform Crime Reporting Division Manager and Statistical Analysis Center Director, Alabama Criminal Justice Information Center

Topics

- ◆ Background of CONNECT
- ◆ States involved and their legal analyses
- ◆ Data shared
- ◆ Performing privacy impact assessments
- ◆ Privacy policy development
- ◆ Justice Reference Architecture Policy Academy
- ◆ Other Global implementations
- ◆ Questions

11:00 a.m. – 12:00 Noon

Justice Use of Social Networking Sites—Privacy Implications

Mr. Boehmer, Judge Capizzi, and Ms. Nancy Kolb, Senior Program Manager, International Association of Chiefs of Police, Community Safety Initiatives and the IACP Center for Social Media

Topics

- ◆ GESC/GAC recommendation
- ◆ Police and law enforcement agency use of social networking sites—right to access
- ◆ Use by litigators to screen jurors
- ◆ IACP Center for Social Media (issue paper, model policy, etc.)

12:00 Noon – 1:30 p.m.

Lunch (on your own)

1:30 p.m. – 1:45 p.m.

Status of Other Privacy Efforts

Ms. Goggins, CONNECT, and Ms. Christina Abernathy, Institute for Intergovernmental Research

Topics

- ◆ Status of NGA Center for Best Practices—Privacy Policy Academy
 - HJIS stakeholder privacy impact assessments, August 10–13, 2010
- ◆ Status of the Fusion Center Privacy Policy Technical Assistance program

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Wednesday, November 17, 2010 (continued)

1:45 p.m. – 3:00 p.m.

Defining Privacy and Related Concepts

Barbara Hurst, Esquire, Rhode Island Office of the Public Defender

Ms. Martha Steketee, Independent Consultant

Topics

- ◆ Privacy Guide drafting session—October 5–6, 2010, Tallahassee, Florida
- ◆ Status of Privacy Guide revisions
- ◆ Exploration of the term “privacy,” when is it implicated, and related concepts
- ◆ Impact on Section 4, Understanding Privacy Concepts, of the Privacy Guide
- ◆ Relevance to other Global products

3:00 p.m. – 3:15 p.m.

Break

3:15 p.m. – 3:45 p.m.

Furthering the GPIQWG Information Quality (IQ) Series

Mr. Stevenson

Topics

- ◆ Piloting the IQ Series with a state agency or program
- ◆ Other IQ tools for development and outreach

3:45 p.m. – 4:45 p.m.

GPIQWG 2011 Draft Business Plan

Judge Capizzi

Topics

- ◆ 2011 proposed GPIQWG priorities
 - Completion/vetting/GAC approval of revised Privacy Guide and companion CD
 - Update of the Privacy Impact Assessment
 - Furthering the IQ Series
 - Denver Familial DNA Search Privacy Policy
 - Privacy principles of familial DNA searching
 - Privacy implications of social networking sites
- ◆ Discussion on other priorities/recommendations

4:45 p.m. – 5:00 p.m.

Next Steps and Closing Remarks

Judge Capizzi

Topics

- ◆ Review of today’s action items
- ◆ Plan for the following day’s GPIQWG meeting

5:00 p.m.

Adjournment

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Thursday, November 18, 2010

- 8:30 a.m. – 8:45 a.m. **Introduction and Charge for the Day**
Judge Capizzi
Topics
- ◆ Welcome
 - **Guest:** Ms. Jennifer Luttmann, Chief, CODIS Unit, Federal Bureau of Investigation Laboratory (bio in meeting packets)
 - ◆ Review of today's goals and charge to the group
- 8:45 a.m. – 9:00 a.m. **DHS Office of Civil Rights and Civil Liberties**
Ms. Ayn Crawley, Director, Civil Liberties Institute, Office of Civil Rights and Civil Liberties, U.S. Department of Homeland Security
Topics
- ◆ Status of state/local fusion center training events
 - ◆ Lessons learned from Year One of fusion center training
- 9:00 a.m. – 10:15 a.m. **Breakout Sessions**
Judge Capizzi
GPIQWG Breakout Groups
- ◆ Denver Familial DNA Privacy Policy—Case Study
 - ◆ Privacy Guide Revisions Task Team
 - ◆ Privacy Implications of Social Networking Task Team
 - ◆ Furthering the IQ Series Task Team
- 10:15 a.m. – 10:30 a.m. **Break**
- 10:30 a.m. – 11:30 a.m. **Breakout Sessions** *(continued)*
- 11:30 a.m. – 11:50 a.m. **GPIQWG Task Team Status Reports**
Judge Capizzi
Topics
- ◆ Denver Familial DNA Privacy Policy—Case Study
 - ◆ Privacy Guide Revisions Task Team
 - ◆ Privacy Implications of Social Networking Task Team
 - ◆ Furthering the IQ Series Task Team

Global Justice Information Sharing Initiative (Global) Privacy and Information Quality Working Group (GPIQWG) Meeting



Embassy Suites DC Convention Center
900 Tenth Street, NW
Washington, DC 20001
(202) 739-2001



United States
Department of Justice

November 17–18, 2010

Capital A Ballroom

Agenda—Thursday, November 18, 2010

11:50 a.m. – 12:00

Noon

Next Steps and Closing Remarks

Judge Capizzi

Topics

- ◆ Review of action items and assignment of tasks
- ◆ Next meeting reminder: February 23–24, 2010, Nashville, Tennessee

12:00 Noon

Adjournment

