

DEVELOPING A CYBERVETTING STRATEGY

FOR LAW ENFORCEMENT



PERSEREC 

Defense Personnel Security Research Center
U.S. Department of Defense

DEVELOPING A CYBERVETTING STRATEGY FOR LAW ENFORCEMENT

SPECIAL REPORT

Andrée Rose
Howard Timm
Corrie Pogson
Jose Gonzalez
Edward Appel
Nancy Kolb

December 2010

CONTENTS

Section 1. Introduction	1
Background	1
Approach	2
How to Use This Document	3
Section 2. Developing a Cybervetting Policy	4
Purpose and Scope	4
Preemployment Screening and Post Hire Monitoring	4
Notice and Consent	5
Lateral Police Transfers	6
Cyber Searches	6
Personnel Authorized to Conduct Cybervetting	6
Employment Application or Background Questionnaire	7
Search Practices	7
Search Restrictions	9
Search Results	9
Training	9
Social Media	9
Social Media Guidelines	13
Monitoring	15
Reporting	15
Review of Data	16
Social Media Training for Personnel	16
Authentication	17
Policy	17
Practices	18
Adjudication	19
Hiring, Retention, Promotion, and Disciplinary Decisions	20
Incumbents	20
Training	21
Safeguarding Data	21
Section 3. Additional Resources	22
Section 4. Acknowledgements	23
Section 5. Glossary	28
Section 6. Notes and Citations	30
Other Sources Consulted	32

Appendix A	Sample Forms	35
Appendix B	Project Participants: Job Sector and Occupation	37
Appendix C	Cybervetting Guidelines	39
	Purpose and Scope	39
	Notice and Consent	39
	Lateral Police Transfers	39
	Cyber Searches	39
	Personnel Authorized to Conduct Cybervetting	39
	Employment Application or Background Questionnaire	39
	Search Practices	39
	Search Restrictions	40
	Search Results	40
	Training	40
	Social Media	40
	Social Media Guidelines	40
	Monitoring	41
	Reporting	41
	Review of Data	41
	Social Media Training for Personnel	41
	Authentication	41
	Policy	41
	Practices	41
	Adjudication	41
	Hiring, Retention, Promotion, and Disciplinary Decisions	41
	Incumbents	41
	Training	41
	Safeguarding Data	42

List of Tables

Table 1. Case Law Concerning Access to Password-Protected Websites via Third-Party Login Credentials	6
Table 2. Case Law on Providing Favorable Evidence to Defense Counsel	10
Table 3. Case Law on the Application of First Amendment Protections to Public Employees	11
Table 4. Case Law on the Application of First Amendment Protections to Law Enforcement Personnel	12
Table 5. Case Law Pertaining to Coworker Harassment in Cyberspace	16
Table 6. Case Law Concerning Online Behavior	20

List of Figures

Figure 1. Fair Credit Reporting Act (FCRA)	5
Figure 2. Passwords	7
Figure 3. What Is a Search Engine?	8
Figure 4. <i>Training Day</i>	9
Figure 5. Stormfront Posting	14
Figure 6. Example of Login Banner	15
Figure 7. A Photo of a Corpse on Facebook	16

Figure 8. Cyber Threats	17
Figure 9. Fraudulent Social Media Profile	17
Figure 10. Reporting Fraudulent Social Networking Accounts	18
Figure 11. Indicators of a Compromised Social Networking Profile	19
Figure 12. Posting Sensitive Information on the Internet	19
Figure 13. Adverse Employment Decisions and the FCRA	21
Figure 14. Equal Treatment	21

List of Tables in Appendices

Table B-1. Cybervetting Project Participants by Job Sector	37
Table B-2. Occupations within the Law Enforcement Sector	37
Table B-3. Occupations within the Other Sectors	38

List of Figures in Appendices

Figure A-1. Sample Preemployment Screening Questionnaire	35
--	----

SECTION 1. INTRODUCTION

Cybervetting is an assessment of a person's suitability to hold a position using information found on the Internet to help make that determination. Cybervetting occurs even though there are no generally accepted guidelines and procedures for fair, complete, and efficient Internet searches for this purpose. Job applicants, employees, and employers are often uncertain whether cybervetting is legal, where privacy rights begin and end, and what cyber behaviors and postings should be subject to cybervetting.

The purpose of this document is to present policies and practices to consider when using the Internet to search for information on law enforcement applicants, candidates, and incumbents, and when developing social media policies to limit inappropriate online behaviors. Cybervetting guidelines need to strike the right balance between individuals' constitutional rights and law enforcement agencies' due diligence responsibilities for screening out undesirable job applicants and employees.

Background

In the mid- to late-2000s, the ease, speed, and cost of electronically searching for information pertaining to a specific person or a group of persons became easier and cheaper because of increased (1) access to the Internet,¹ (2) availability of search engines, (3) availability of public records on the Internet, and (4) popularity of social media and video sharing websites.

As social media gains prominence in the cyber arena, its effects are also felt in the brick and mortar environment. Within law enforcement, many of the spillover effects have been of significant consequence. User-generated content is used by attorneys to impeach officer testimony and to support claims of negligent hiring and retention of police officers.² Additionally, police officer misconduct involving online and mobile communications has contributed to an increase in sexual harassment lawsuits.³ From a personal safety perspective, the Internet provides offenders with instantaneous access to information about law enforcement personnel and their families who choose to have a web presence. In response to these concerns, many law enforcement administrators are reviewing information found online to supplement pre-employment screening and post hire monitoring.

Using the Internet to gather information concerning job applicants and incumbents is an extension of existing background investigations conducted on persons applying for positions and promotions within law enforcement. The Internet is merely a new source to identify and collect information about people's behavior. The critical difference is that much of what people do today is done on the Internet. People need to be trustworthy

and responsible in that medium as well as in the physical world. At its core, the purpose of cybervetting is to ensure that (1) the person being considered is trustworthy, (2) the individual has behaved in a manner consistent with law enforcement mores, and (3) if the person has not behaved in an appropriate manner, his or her future online and offline behavior is likely to become and remain acceptable through training, maturation, and supervision.

When implemented within the framework of the law, cybervetting has the potential to yield a number of benefits to law enforcement. First, cybervetting should increase public confidence in the professionalism of policing by reducing the number and magnitude of inappropriate behaviors attributed to law enforcement personnel. Furthermore, Internet search results may

1. corroborate or contradict information provided on a resume or job application;
2. identify candidates and employees who posted text, audio, or images that
 - a. contain sensitive law enforcement information,
 - b. reflect a subject has engaged in criminal or status offenses,
 - c. indicate a subject is associated with hate, criminal, or terrorist organizations, or
 - d. reflect a subject is a danger to self or others.

Law enforcement agencies must exercise caution when developing, implementing, and monitoring these types of policies. The following legal, ethical, practical, and technical issues must be considered.

1. Employers may be in danger of acquiring certain types of information that hampers rather than helps effective, efficient, and appropriate personnel practices.
 - a. Information pertaining to protected classes⁴ may have been posted by applicants or employees or inferred based on the websites where they have participated (for example, <http://www.outeverywhere.com> and <http://www.blackplanet.com>).
2. Failure to examine and consider case law when developing cybervetting may lead to violations of the U.S. Constitution, such as the provisions applicable to freedom of speech and assembly.
3. False positives may occur, such as basing adverse employment decisions on Internet information that is applicable to another person or that was falsely manufactured to harm the person under review.
4. Employers may limit their acquisition and retention of talent by
 - a. overreacting to trivial indiscretions,⁵
 - b. applying cybervetting practices that are irrelevant for predicting future behavior, or
 - c. accepting too many false positives due to widespread inaccurate information in cyberspace.

5. Cybervetting is likely to add to the cost and duration of the background investigation and continuing evaluation process.

Approach

This project was a collaborative effort between the International Association of Chiefs of Police (IACP), the Defense Personnel Security Research Center (PERSEREC), and hundreds of subject matter experts (SME) and stakeholders to develop policies and procedures for vetting and monitoring cyber behaviors and postings of prospective employees, incumbents, and national security clearance holders. The guidelines presented in this document pertain to law enforcement; cybervetting guidelines for national security positions are provided in a separate report.⁶

To create effective, efficient, and just cybervetting guidelines, this project set out to identify (1) boundaries where subjects' reasonable expectations of privacy end and where the government's due diligence responsibility for monitoring and investigating people holding or seeking sensitive positions begins, (2) common standards of proof regarding identifying the person who actually engaged in the cyber behavior of concern, and (3) the most effective, efficient, and appropriate means for collecting and adjudicating cyber posting/behavior information.

The first step toward developing relevant and useful guidelines was to conduct a literature review on (1) the use of online information when making employment decisions, (2) social media policies, and (3) relevant employment law. Cybervetting recommendations were culled from a variety of sources, including peer-reviewed articles, agency and organization reports, journalistic reports, and government and private sector cyber-related policies. In addition, presentations about the project were made to the ASIS Defense and Intelligence Council and the Institute for Law Enforcement Administration. Members of the audience were asked to share their organizations' cybervetting and social media policies and procedures with the research team.

The literature review produced a set of strawman proposals and also provided names of SMEs—people with in-depth knowledge and experience in related areas. We were most interested in SMEs who were experienced professionals in one or more of the following fields:

- law enforcement administration
- national security
- preemployment screening and background investigations
- employment recruitment and selection
- employment law
- privacy
- open-source intelligence
- social media and blogging

The second step was to interview a subset of the identified SMEs. During these interviews, SMEs were asked to (1) list the pros and cons associated with cybervetting, (2) identify specific practices that should be used or avoided, (3) define public and private online information, (4) identify legal and privacy concerns, and (5) provide names of other SMEs.

Strawman proposals from the literature review and results from SME interviews were used to craft an online survey hosted by the IACP. The survey was developed to gather feedback from SMEs and stakeholders about the cybervetting policies and practices. PERSEREC and IACP wanted to learn more about the perceived utility, practicality, and legality of these policies and practices. Survey participants were asked to read each survey item and indicate if they (1) agree, (2) agree only if the item is modified, or (3) disagree. Participants were also given the opportunity to describe how they would modify the item.

The first draft of the cybervetting guidelines was created based on the survey results. Survey items with a high degree of disagreement were discarded, while most other items were modified using the suggestions provided by survey respondents. These guidelines were then presented at 16 focus groups. A focus group is a qualitative research method in which a moderator directs a small group of people in an interactive discussion designed to elicit opinions and perceptions about a specific topic. These groups consisted of SMEs, stakeholders, and affected practitioners. Specifically, sworn law enforcement personnel, cadets, academics, human resource specialists, employment lawyers, technology experts, privacy advocates, recruiters, bloggers, security managers, background investigators, fraud investigators, private sector representatives, and city, state, and federal officials attended these focus groups.⁷

The focus groups were designed to bring an array of professionals to the table, because (1) the data of interest pertained to two employment sectors and (2) the development of lawful and just cybervetting guidelines benefited from input from a diverse group of professionals. For example, employment lawyers provided comments pertaining to what Internet-related information could and should be asked on a job application; privacy advocates shared concerns about accessing information that employers should not be using to make employment decisions; and background investigators provided information on the investigative process and explained how useful information from the Internet could be retrieved during the investigative stage of the employment and security clearance processes.

The guidelines initially consisted of more than 100 specific items. Due to time and participant limitations, we were not able to cover each item in every focus group. The items that were covered were subject to revision based on the group's feedback.⁸ Group moderators attempted to achieve consensus on each item, and when consensus could not be reached, a vote was taken. The suggested revision with the most votes moved on to the next focus group. When a group suggested that an item be stricken, the item was carried over to the next focus group for their opinion. After two focus groups indicated that an item should be stricken, the item was removed from the proposed guidelines. However, if a deleted item was brought up at subsequent focus groups, it was reintroduced into the guidelines for additional consideration.

Items were added to the guidelines when focus groups suggested policies or procedures not already covered. Some agencies provided their cyber-related policies after having a representative attend a focus group. Practices not already included in the project's guidelines were added and vetted at subsequent focus groups.

Two exceptions were made to this methodology. If an item was selected for deletion in both Groups 14 and 15, the item was carried over to Group 16, the capstone focus group. Group 16 discussed the merits and concerns about the item and decided whether or not the item would remain in the guidelines. The purpose of this exception was to prevent items that withstood multiple focus groups from being eliminated without due consideration.

The second methodological exception only concerned Group 16. This group reviewed every item listed within the guidelines and suggested one new item (item is noted within the report). Group 16 also suggested more descriptive text be added to the report in order to provide context to some of the items within the guidelines.

Focus groups were hosted by local agencies or companies. They supplied meeting space, audio/visual equipment, and refreshments. The names of SMEs and focus group participants who donated their time and expertise to this project are listed in the acknowledgments section of this report.

Focus groups 1–15 were held in the following locations:

- Monterey, California
- Redmond, Washington
- Plano, Texas (2)
- Baltimore, Maryland
- St. Paul, Minnesota
- Falls Church, Virginia
- Chicago, Illinois
- Akron, Ohio
- Denver, Colorado
- Wayne, New Jersey
- Atlanta, Georgia
- Boston, Massachusetts
- Orlando, Florida
- Toronto, Ontario

The draft guidelines that resulted from these meetings were reviewed and revised at the capstone focus group, hosted by the IACP, in Alexandria, Virginia. Focus group hosts,⁹ and personnel from the IACP and PERSEREC attended this meeting.

As a result of this collective effort, guidelines for effectively, efficiently, and fairly searching the Internet to obtain information on job applicants and employees are provided in this document. The following areas are addressed:

- Cybervetting – an assessment of a person's suitability to hold a position using information found on the Internet.
- Social media – policies and practices designed to limit employees' ability to expose their agencies to increased liability by degrading their agencies' image through inappropriate online behavior, or to endanger themselves or their families by posting information that could be misused by others.
- Authentication – an assessment of the validity and reliability of data obtained from the Internet.
- Adjudication – an assessment of an individual's reliability, trustworthiness, and fitness to serve in a position of trust.

How to Use This Document

These guidelines were designed to provide law enforcement executives with information they need in order to develop solutions that address the needs of their community. They do not represent a "suggested" or "model" solution that law enforcement agencies are recommended to follow.

Each law enforcement agency operates in a unique environment of federal, district, and appellate court rulings, state laws, local ordinances, regulations, judicial and administrative decisions, and collective-bargaining agreements that must be considered by a chief while designing policies and procedures for their department.

In addition, the formulation of specific agency policies must take into account local, political, and community perspectives and customs, prerogatives, and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors.

Section 2 contains guidelines that law enforcement agencies should consider when developing a cybervetting policy. Some of the draft policies presented may be applicable to the department without modification. Others may not be applicable at all or only with modification. Additional policies not included in this document may need to be added. It is hoped that the guidelines presented will serve as a good starting place for law enforcement agencies interested in establishing cybervetting policies.

Each section of this report contains additional useful information such as important facts, case law,¹⁰ and anecdotes of social media in the workplace. Section 3 provides a list of additional resources that may be useful when formulating policy.

Key terms within this document are hyperlinked to definitions within the glossary located in Section 5. It should be noted that there are hundreds of social networking sites and each uses unique terms for describing similar acts and functions. For example, the Facebook phrase "friend request" refers to the act of asking someone to be one's friend. LinkedIn uses the phrase "invite to connect" to add someone to one's professional network, and Twitter users "follow" other users. For the sake of consistency and ease of reading, this report often uses Facebook terminology. This language was selected because Facebook has more than 500 million active users,¹¹ more users than any other social networking site.

Appendix A contains a sample consent form and supplemental background questionnaire. Appendix B presents the types of professionals who participated in this project. Appendix C contains the cybervetting guidelines without accompanying text.

Finally, it should be noted that this document was written with U.S. law enforcement agencies in mind, specifically, state, local, and tribal law enforcement agencies. Federal law enforcement agencies interested in establishing cybervetting policies and procedures are encouraged to utilize both this document and its companion report.¹²

SECTION 2. DEVELOPING A CYBERVETTING POLICY

Increasingly, employers are searching the Internet for information on potential recruits¹³ and existing employees. Furthermore, a recent research effort sponsored by the Microsoft Corporation found that 70 percent of U.S. recruiters and human resource professionals decided not to hire candidates because of information they found online.¹⁴

Problems such as invading privacy and using inaccurate information to make employment decisions may arise when agencies use online content without a clear and well-thought-out organizational policy for doing so. The following section is designed to help agencies develop a lawful and enforceable cybervetting program that meets its specific needs.

When developing a cybervetting policy, policy makers must take into consideration a number of factors, such as the following:

- The purpose and scope of cybervetting.
- At what stage during the hiring process should cybervetting occur? At what stages during employment should cybervetting occur?
- Should notice of cybervetting be given to those being vetted?
- Is consent required?
- What are the requirements for personnel conducting Internet searches?
- What personal information will be used to facilitate a complete and accurate cyber investigation?
- What are appropriate cybervetting methods?
- How will cybervetting results be authenticated?
- How should decision makers adjudicate cybervetting results?
- How will cybervetting results be protected from unauthorized disclosure?
- What are the potential political and resource costs from deciding to implement or not implement cybervetting?
- What will be the resource impact of adding this type of vetting?

Purpose and Scope

This section of the report provides general guidance on developing a cybervetting policy.

1. Law enforcement agencies should create a cybervetting policy that describes the purpose and scope of cybervetting. The policy should include information on the general types of information checked, collected, and used. This policy should be
 - a. applied uniformly to all applicants, candidates, and incumbents;

- b. reviewed periodically by management and updated as needed;
 - c. reviewed and approved by the agency's legal counsel; and
 - d. made available to the public.
2. An agency's cybervetting policy should also apply to third parties who engage in work on behalf of that agency. Organizations that provide policing services (for example, 9-1-1 dispatching or background investigations) should contractually agree to maintain consistency with the cyber-related policies an agency has in effect.¹⁵

Preemployment Screening and Post Hire Monitoring

With respect to preemployment screening, an agency must decide at which point within the hiring process it is most advantageous to cybervet. The decision to search the Internet for information on an applicant or a candidate will be based on a series of factors including the size of the applicant pool, the number of qualified applicants, the number of candidates, the cost of conducting the check, its productivity in identifying issues of concern, the accuracy and reliability of information found during the check, the agency resources and budget, the components of the planned cybervetting program, and the costs associated with other available preemployment screening techniques and systems.

The cost and extent to which agencies can disqualify applicants from employment because of online behaviors or other online information, as well as the accuracy and reliability of that information, will affect when those checks should be conducted in the selection process. If the measures that eliminate the most applicants per dollar spent are applied first, and those measures are based on authenticated information, the department may be able to reduce costs by not having to pay for other elements of the selection process (for example, physical fitness exams, psychological and polygraph tests, and background investigations) and do so in a legally defensible manner. However, cybervetting applicants can be time consuming and expensive, especially if agencies have large pools of applicants. Agencies with a large applicant pool may find it too expensive to cybervet all applicants.

Depending on how a cybervetting program is structured, conducting searches on candidates rather than applicants may require fewer resources because the candidate pools are often much smaller than the original applicant pools. However, agencies run the risk of disqualifying a candidate because of

online information after having paid for the candidate to undergo a battery of checks, tests, and evaluations.

Agencies must also decide when it is most appropriate to conduct searches on incumbents. Staffing, budget, and other resource considerations may affect how often these searches are conducted on employees. Agencies may want to conduct cyber searches on employees when (1) they become aware of cyber behavior or postings that are in violation of existing policies, (2) when an employee is considered for promotion, (3) when retention and disciplinary decisions are made, or (4) when a specified length of time has passed since the last time that person was cybervetted.

Notice and Consent

During focus group discussions, many participants indicated that notice and consent are important components of the cybervetting process. Notice protects privacy by allowing job applicants to make informed decisions about the collection and use of their personal, albeit publicly available, information and self-select out of the hiring process. However, law enforcement

agencies that want to incorporate cybervetting into their background investigations are not legally required to inform job applicants, candidates, or incumbents about employment-related cybervetting unless those searches are performed by a third party (see Figure 1).

Obtaining consent is essential if an agency intends to gather information from a website, social networking profile, or other cyber source protected by a password. Table 1 summarizes case law pertaining to unauthorized access to password-protected websites as well as the permissible use of third party login credentials to access these sites. This is an emerging area of case law. Agencies that engage in cybervetting should stay abreast of court rulings relating to employment and social media and be prepared to modify their cybervetting strategies in accordance with these rulings.

Lastly, law enforcement executives should also be aware that consent may be required when collecting personally identifying and publicly available data housed on servers in other countries. Privacy laws and regulations in Europe, Canada, and Asia are

15 U.S.C. § 1681 regulates the collection, dissemination, and use of consumer information, including consumer credit information. The Fair Credit Reporting Act (FCRA) also covers investigative consumer reports.

A consumer report contains information about your personal and credit characteristics, character, general reputation, and lifestyle. To be covered by the FCRA, a report must be prepared by a consumer reporting agency (CRA) — a business that assembles such reports for other businesses...investigative consumer reports — reports that include interviews with an applicant's or employee's friends, neighbors, and associates. All of these types of reports are consumer reports if they are obtained from a CRA.¹⁶

Law enforcement agencies using third parties to conduct Cyber searches for cybervetting purposes will need to adhere to the following requirements:

15 U.S.C. 1681d

(a) *Disclosure of fact of preparation.* A person may not procure or cause to be prepared an investigative consumer report on any consumer unless:

(1) It is clearly and accurately disclosed to the consumer that an investigative consumer report including information as to his character, general reputation, personal characteristics, and mode of living, whichever are applicable, may be made ...

(b) *Disclosure on request of nature and scope of investigation.* Any person who procures or causes to be prepared an investigative consumer report on any consumer shall, upon written request made by the consumer,... make a complete and accurate disclosure of the nature and scope of the investigation requested.

In other words, if law enforcement agencies use third parties to perform cybervetting functions they will need to inform anyone who might be cybervetted that this type of investigation may be conducted.

The FCRA does not apply to (1) investigations conducted by an employer's personnel, or (2) when a third party, whose primary business is something other than providing such reports, conducts the investigation.¹⁷

FIGURE 1. FAIR CREDIT REPORTING ACT (FCRA)

TABLE I. CASE LAW CONCERNING ACCESS TO PASSWORD-PROTECTED WEBSITES VIA THIRD-PARTY LOGIN CREDENTIALS

<i>Case</i>	<i>Background</i>	<i>Ruling</i>
<p><i>Pietrylo v. Hillstone Restaurant Group</i>, Docket No. 2:06-cv-05754 (D.N.J. 2008)</p>	<p>Two employees were terminated by the Hillstone Restaurant Group for posting derogatory comments on a password-protected MySpace page. The lawsuit claimed the restaurant’s managers “strong-armed and threatened a member of the private group so that this member was forced into providing them with the member’s e-mail address and password.”</p>	<p>June 2009: A jury found that the restaurant’s managers “violated the Stored Communications Act and the New Jersey Wire Tapping and Electronic Surveillance Act by accessing the MySpace page without authorization.” With respect to the invasion of privacy claim, “the jury found that the plaintiffs had no reasonable expectation to privacy on MySpace.”¹⁸</p> <p>September 2009: The Federal District Court of New Jersey upheld the jury’s verdict. Hillstone Restaurant Group was held liable for violations of the Stored Communications Act, 18 U.S.C. §§ 2701-2710, and New Jersey’s electronic surveillance statute.</p>
<p><i>Konop v. Hawaiian Airlines, Inc.</i>, 302 F.3d 868, 885 (9th Cir. 2002)</p>	<p>The plaintiff, a pilot for Hawaiian Airlines, created a password-protected website critical of Hawaiian Airlines’ president and union.</p> <p>The Hawaiian Airlines Vice President (VP), without the plaintiff’s authorization, accessed the website using another pilot’s username and password. However, the authorized user had never before accessed the website.</p> <p>The plaintiff also claimed the VP disclosed the contents of the website to Hawaiian Airline’s president and the Air Line Pilots Association.</p> <p>The VP accessed the website a second time by using the name and password of another pilot. This pilot had previously accessed the website and consented to the VP’s use of his login credentials.</p>	<p>Ninth Circuit Court ruled that the unauthorized access and review of the contents on a password-protected website can constitute violations of the Wiretap Act, 18 U.S.C. §§ 2510-2520, and the Stored Communications Act, 18 U.S.C. §§ 2701-2710.</p> <p>The court also “held that the Stored Communications Act authorizes users of a website to give permission to others to access the website, but must actually access the website to be a “user;” absent access, the person has no authority to authorize a third party to access the website.”¹⁹</p>

protective of personally identifying data, requiring public and private record holders to allow users to opt in before the records can be collected and/or disclosed.²⁰

Chief executives may want to incorporate the following notice and consent guidelines into agency cybervetting policies:

1. Law enforcement agencies shall inform applicants, candidates, and incumbents, in writing, that the Internet may be used to search for relevant information on them and that relevant online information may be collected and used to make employment decisions.
2. With applicants’, candidates’, and incumbents’ consent, law enforcement agencies may review online information about these individuals available on websites where a subject’s password is required to view content.
3. Applicants, candidates, and incumbents should be notified that failure to provide consent and/or deliberate concealment of or prevention of access to online content may impact on their employment status.

Lateral Police Transfers

Focus group participants expressed concern that an agency seeking to hire additional personnel might not be willing or able to share disqualifying information discovered during the cybervetting process with a lateral applicant’s current employer without first obtaining consent from the applicant. The following item was drafted in an effort to address this concern:

1. Law enforcement agencies should notify lateral applicants that any information that is of a public safety concern or reflects upon their fitness for the position of a police officer may be shared with their current employer if the chief executive or designee at the agency conducting the vetting deems it necessary.

Cyber Searches

Personnel Authorized to Conduct Cybervetting

Comments made during one focus group indicated that some agencies are using college interns to search the Internet for

information on job candidates. While the intern may know how to navigate the Internet and social media better than most, he or she is acting in this case as a human resource investigator. This type of investigator should be someone whose background indicates that he or she is suitable for access to personal information.

1. Personnel authorized to conduct cybervetting should be classified as holding a sensitive position and vetted in accordance with that classification.
2. Personnel authorized to conduct cybervetting should be notified that information collected from the Internet is confidential.

Employment Application or Background Questionnaire

The employment application or background questionnaire can be used to collect personal information needed to conduct a thorough Internet search on potential employees and incumbents. For example, some personal information may be used as search terms, while other information may be used to mitigate or refute search results. Law enforcement agencies that plan or are already cybervetting prospective employees should consider incorporating the following questions into their employment applications or background questionnaires:

1. The employment application or background questionnaire should ask job applicants, candidates, or incumbents:
 - a. For any e-mail addresses they have used over a period of time (period of time to be determined by the agency and the scope of its investigation). They should be notified that e-mail addresses will be used as search terms and that they are not required to disclose legally restricted e-mail addresses (for example, undercover or classified e-mail addresses).
 - b. For online screen names, handles, or nicknames used over a period of time (period of time to be determined by the agency and the scope of its investigation). They should be notified that screen names, handles, and nicknames will be used as search terms. Requests should be limited to usernames and should not include information such as login credentials for online health care and banking.
 - c. For the websites or blogs where they are members, where they frequent, or where they contribute.

- d. About any electronic content that would suggest a conflict of interest or could reflect negatively upon themselves or the potential employer. They should be afforded the opportunity to explain any potential concern.
 - e. If they have ever been a victim of identity theft, cyber bullying, or malicious postings. They should be afforded the opportunity to explain any potential concern they think might surface during the cybervetting process.
2. Law enforcement agencies should not ask for passwords. See Figure 2 for information on one city's attempt to ask job applicants for passwords.

Search Practices

The cybervetting practices suggested below are those practices that were agreed upon in the focus groups. An agency's search techniques should not be limited to the items in this section because as technology progresses, new and more efficient search methods will likely become available.

1. Before drafting cybervetting practices, an agency should first ensure that policy makers know how social media tools work. Decision makers should stay abreast of policy and technical changes made by social networking sites.

How does Social Media Work?

Comments from the focus groups indicated that some agencies are asking candidates with Facebook accounts to accept a friend request from someone within the agency. This allows the agency to review candidates' profiles without having to ask them to 1) provide passwords or 2) sign into their profiles in the presence of a recruiter or background investigator. While this may initially appear to be a successful work-around solution, Facebook's privacy settings allow someone to accept a friend request and limit the content that a given friend can access. For example, Facebook allows its users to post multiple photo albums, and each of those photo albums can be shared with or hidden from specific friends.

For additional information on social media, visit the IACP's *Social Media Fact Sheet* at <http://www.IACPsocialmedia.org>.

In 2009, officials in Bozeman, Montana, asked job applicants to list all user names and passwords for "any Internet-based chat rooms, social clubs, or forums to include but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc." Officials claimed this information helped them complete a thorough background investigation. Nonetheless, the city suspended this practice after widespread outrage, noting "it appears to have exceeded that which is acceptable to our community."²¹ A poll indicated that 98 percent of respondents believed that asking for passwords is an invasion of privacy.²²

Asking for user names and passwords may create risks more serious than public relations issues. Employers who ask for this information may be held liable when (1) job candidates use the same password for multiple websites (for example, online banking, airline frequent flyer accounts) and (2) they incur a harm or cost at a website that can be accessed using the same user name and password provided to the employer.

FIGURE 2. PASSWORDS

2. Before drafting cybervetting practices, an agency should first ensure that policy makers know how cyber search tools work (for example, search engines and metasearches). See Figure 3.
3. Applicants, candidates, and incumbents may be asked to access password-protected websites so that the recruiter or background investigator can review their profiles, blogs, or other online forums for disqualifying content.
4. Personnel conducting background investigations, including cybervetting, may contact any of the applicants', candidates', or incumbents' associates, including online friends.
5. E-mail addresses may be used as cyber search terms.
6. Screen names, handles, or nicknames may be used as cyber search terms.

Developed Reference

Multiple focus groups indicated that contacting online friends is analogous to contacting developed references, a search method used in traditional background investigations. A developed reference is someone who is identified by a background investigator as having a relationship with the subject of interest but was not identified as a reference by the subject.

A search engine is a computer program that uses a spider or web crawler to scour the World Wide Web for information and then indexes that information. When a user conducts a keyword query, the search engine displays links to websites, images, and other types of files stored in its indexes. A list of search engines is provided to demonstrate the availability of specialized search engines. This list is not exhaustive, nor is it an endorsement.

A Word of Caution

Did you know that search engines may return different results for the same keyword search? For example, Google queries may produce different results because (1) each query is routed to the nearest Google data center and each center may contain different collections of indexed pages, (2) Google alters search results based on one's geographic location, and (3) searches conducted while signed into a Google account will be personalized based on one's search history.²³

Examples of Available Search Engines by Area of Interest

General

Ask.com
Bing
Yahoo! Search
Google

Business

Business.com
GenieKnows
Nexis (Lexis Nexis)
Thomasnet

Mobile/Handheld

Taptu

Job

CareerBuilder
Craigslist
Monster

Legal

WestLaw
Lexis (Lexis Nexis)
USlaw
Quicklaw

News

Google News
Yahoo! News
Nexis (Lexis Nexis)
Topix.net

People

PeekYou
Spokeo
Zabasearch.com
ZoomInfo

Forum

Omgili

Blog

Amatomu
Bloglines
BlogScope
IceRocket

Real Property

HotPads.com
Rightmove
Zillow.com

Multimedia

Bing Videos
Google Video
Yahoo! Video
YouTube

Maps

Wiki Mapia
Bing Maps
Google Maps
MapQuest

E-mail

TEK

Question & Answer

Answers.com
eHow
DeeperWeb

Visual

ChunkIt!
Grokker
Pixsta
PubGene

FIGURE 3. WHAT IS A SEARCH ENGINE?

Search Restrictions

1. Cybervetting may only be conducted on authorized workstations.
2. Cybervetting may not unlawfully bypass applicants', candidates', or incumbents' privacy settings on social networking sites.
3. Personnel conducting cybervetting shall use appropriate representations to obtain online information.

Search Results

The following items concern how cybervetting results should be documented and used:

1. Personnel authorized to conduct cybervetting shall document cyber search methods and results.
2. Cybervetting results supplement background investigations and should be incorporated into the normal, lawful employment process.
3. Law enforcement agencies shall follow existing procedures that ensure information relating or pertaining to protected classes does not negatively impact hiring decisions.

Protecting Protected Classes

If existing procedures are not compatible with cybervetting, this concern may be addressed by compartmentalizing the process. For example, a non-decision maker can conduct cyber searches and provide the hiring manager with search results that have been stripped of protected class data (Sprague, 2007; Jackson, 2009).

4. Law enforcement agencies will report evidence of criminal activity uncovered during the cybervetting process to the

appropriate law enforcement agency when doing so is consistent with existing policies or as required by law.

Training

Law enforcement agencies should ensure that appropriate training and mentoring is provided to all personnel involved in the cybervetting process (for example, policy makers, decision makers, and investigators). Training should address the following legal, ethical, and technical areas:

1. Scope and purpose of cybervetting,
2. Guidance on using Internet and social media tools,
3. Capturing and retaining relevant information,
4. What constitutes prohibited grounds for discrimination, and
5. Safeguarding data.

Social Media

Social media provides a window into the life of each user. Sometimes users choose to present their personal life, while others share their professional lives. More commonly, they are providing a glimpse into both. With respect to law enforcement, this glimpse has provided defense attorneys with an opportunity to access information that may call in question arresting officers' credibility, which may be introduced as evidence during the trial.

For example, Figure 4 tells the story of a New York police officer whose testimony was impeached when a defense attorney introduced the officer's off-duty cyber postings into evidence during the criminal trial of a suspect arrested by the officer. When a police officer's testimony is impeached, it may (1) influence the outcome of the criminal trial; (2) affect past and pending criminal cases, depending on the role the officer played and the strength of the case without the officer's testimony;²⁴ and (3) diminish the officer's value to the police department because he or she can no longer testify in court.²⁵

In 2009, a police officer and frequent poster provided testimony against a parolee the officer arrested. The defendant was charged with felony possession of a handgun and ammunition. When the case went to trial the officer found himself confronted by a defense attorney yielding excerpts from his MySpace account. "[Officer's name] is watching *Training Day* to brush up on proper police procedure." This is a reference to a 2001 movie portraying a corrupt Los Angeles police detective. Additional online comments, also belonging to the officer, describe roughing up a cuffed suspect.

The defense team's strategy focused on the officer's workplace suspension for testing positive for steroids. The defense argued that the officer's use of steroids caused him to go into a rage and assault the defendant. In an effort to justify excessive force, the officer planted a 9-millimeter Beretta on the defendant. The online statements posted by the officer were presented to the court in support of the defense's theory.

The defendant was acquitted of the felony possession charge but found guilty of resisting arrest. The officer later opined that he was partially responsible for the acquittal. "It paints a picture of a person who could be overly aggressive."²⁶

An examination of the officer's online behavior at either the recruitment or promotion phases may have identified a conflict of interest or other possible issues.

FIGURE 4. TRAINING DAY

TABLE 2. CASE LAW ON PROVIDING FAVORABLE EVIDENCE TO DEFENSE COUNSEL

Case	Background	Ruling
<i>Giglio v. United States</i> , 405 U.S. 150 (1972)	“Petitioner filed a motion for a new trial on the basis of newly discovered evidence contending that the government failed to disclose an alleged promise of leniency made to its key witness in return for his testimony. At a hearing on this motion, the Assistant United States Attorney who presented the case to the grand jury admitted that he promised the witness that he would not be prosecuted if he testified before the grand jury and at trial. The Assistant who tried the case was unaware of the promise.”	The U.S. Supreme Court extends the <i>Brady</i> rule and finds that the prosecution must provide defense counsel with any information germane to the credibility of the prosecution’s witnesses. Furthermore, both the prosecution and the police must make an effort to discover information that speaks to a witness’s credibility.
<i>Brady v. Maryland</i> , 373 U.S. 83 (1963)	“... petitioner and a companion were convicted of first-degree murder and sentenced to death. At his trial, petitioner admitted participating in the crime, but claimed that his companion did the actual killing.” Prior to the trial, the petitioner’s attorney requested the companion’s extrajudicial statements. Statements were provided except for one in which the companion admitted to being the sole executioner.	The Court found that police departments have an affirmative duty to provide both the prosecution and the defense with information that is exculpatory for the accused, could mitigate the offense, or affect the severity of the sentence. ²⁸ “Suppression by the prosecution of evidence favorable to an accused who has requested it violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.”

Because the Internet is now a source of user-generated content, it is a medium where police and prosecution should be looking for information on government witnesses. Table 2 presents case law pertaining to the credibility of government witnesses. In *Brady v. Maryland*, the U.S. Supreme Court ruled that police departments must provide the prosecution and defense with exculpatory or mitigating information. The Court’s decision in *Giglio v. United States* builds upon this ruling by requiring police and prosecution to make an effort to find information concerning government witnesses’ credibility (see IACP’s Social Networking and Freedom of Speech Training Key #641).²⁷

When developing social media guidelines, law enforcement agencies will have to bear in mind protections afforded by the U.S. Constitution, namely the First Amendment right to free speech. The U.S. Supreme Court, however, provides guidance on public employees’ rights to free speech through its rulings (see Table 3). A landmark case, *Pickering v. Board of Education*, 391 U.S. 563 (1968), resulted in a ruling that recognized the state’s need to maintain order and efficiency. The Court stated a public employee’s “interest as a citizen in making public comment must be balanced against the State’s interest in promoting the efficiency of its employees’ public services.” The ruling, often referred to as the *Pickering Test*, has implications for law enforcement. The rights of police officers must be balanced against the administration’s concerns about order and discipline

in the workplace. When an officer’s speech harms the police department or its mission, the department may respond as it deems necessary, including terminating the officer.²⁹

Following the *Pickering* case, the Court ruled that the First Amendment protects public employees’ speech when the speech pertains to a matter of public concern, in *Connick v. Myers*, 461 U.S. 138, 146. With respect to disciplining or restricting speech, law enforcement agencies will need to evaluate if the subject of the speech was a matter of public concern or if the officer’s right to free speech is more important than the agency’s efficient operation. Table 3 contains a summary of this case and other relevant court rulings on public employees’ right to free speech.

Table 4 presents additional court rulings concerning the application of First Amendment protections to law enforcement personnel. Many of the outcomes listed in Table 4 use the *Pickering Test* or speech as a matter of public concern as the basis for the rulings.

With respect to police officers, cyber postings often present complex problems that place a fine line between constitutionally protected rights, such as freedom of speech and association, and legal and necessary restrictions on certain expressions of those rights. For example, the white supremacist website Stormfront provides forums where

TABLE 3. CASE LAW ON THE APPLICATION OF FIRST AMENDMENT PROTECTIONS TO PUBLIC EMPLOYEES

<i>Public Employees and their First Amendment Right to Free Speech</i>		
<i>Case</i>	<i>Background</i>	<i>Ruling</i>
<i>Snyder v. Millersville University et al.</i> , 2:2007cv01660 (2008)	<p>In 2006, Stacy Snyder, a 25-year-old student teacher, posted a picture on her MySpace profile that showed her in a pirate costume and drinking from a cup. The caption under the photo read ‘Drunken Pirate.’ Officials at Snyder’s university, Millersville University School of Education, asserted that her MySpace profile promoted drinking and prevented her from receiving a teaching degree.</p> <p>Snyder sued and claimed the university infringed on her First Amendment right to free expression.</p>	<p>The federal district judge ruled that Snyder’s student teacher position made her a public employee. Therefore, the protections afforded to her under the First Amendment are more limited than if she were merely a student. The judge found that Snyder’s ‘Drunken Pirate’ picture was not a matter of public concern. Therefore the school did not infringe upon her right to free expression.</p>
<i>Garcetti v. Ceballos</i> , #04-473, 547 U.S. 410, 126 S. Ct. 1951 (2006)	<p>Ceballos, a deputy district attorney, reviewed an affidavit used to obtain a search warrant and concluded that the affidavit contained errors and misrepresentations. Ceballos informed his supervisors of his findings and drafted a memo recommending the case be dismissed.</p> <p>The deputy district attorney claimed he was subjected to retaliatory actions by his supervisors because of his memo. He filed suit, claiming violation of the First and Fourteenth Amendments.</p>	<p>The U.S. Supreme Court ruled that speech made in an official capacity is not protected by the U.S. Constitution. Justice Anthony Kennedy wrote, “We hold that when public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.”</p>
<i>City of San Diego v. Roe</i> , 543 U.S. 77 (2004)	<p>John Roe, a San Diego police officer, manufactured sex videos of himself stripping off a police uniform and sold the videos on eBay. The city terminated Roe and he responded by suing the city in federal district court. Roe asserted that his termination was in violation of the First Amendment.</p>	<p>The Supreme Court found that Roe’s termination was not in violation of the First Amendment. Government employers can limit their employees’ speech in ways that would ordinarily be unconstitutional. However, government employees are protected by the First Amendment when their speech pertains to matters of public concern. Roe’s speech did not inform the public about a matter of public concern. Furthermore his behaviors were detrimental to the police department.³⁰</p>
<i>Connick v. Myers</i> , 461 U.S. 133, 146 (1983)	<p>Sheila Myers was employed as an Assistant District Attorney. When the District Attorney wanted to transfer Myers to a different section of the criminal court, she opposed the transfer. Myers created and distributed a questionnaire concerning office policies, office morale, confidence in supervisors, and whether employees felt pressured to work in political campaigns. The District Attorney terminated Myers’s employment for refusal to accept the transfer, and also told her that her distribution of the questionnaire was considered an act of insubordination. Myers filed suit claiming wrongful termination because she had exercised her constitutionally protected right of free speech.</p>	<p>The District Court agreed with Myers. The District Attorney was ordered to reinstate her employment and Myers was awarded back pay, damages, and attorney’s fees. The court found that the questionnaire was the primary reason for Myers’s termination, and the questionnaire involved matters of public concern and that there was little evidence to support the claim that the questionnaire interfered with the operation of the District Attorney’s office. The court of appeals affirmed. The U.S. Supreme Court found that a public employee’s speech is protected if it involves a matter of public concern and does not disrupt the workplace. The high court ruled that the District Attorney did not violate Myers’s First Amendment rights when he discharged her for distributing a questionnaire to her fellow assistant district attorneys in the office. Justice Byron White wrote, “Indeed, the questionnaire, if released to the public, would convey no information at all, other than the fact that a single employee is upset with the status quo.”</p>

(continued)

TABLE 3. CASE LAW ON THE APPLICATION OF FIRST AMENDMENT PROTECTIONS TO PUBLIC EMPLOYEES (CONTINUED)

<i>Public Employees and their First Amendment Right to Free Speech</i>		
<i>Case</i>	<i>Background</i>	<i>Ruling</i>
<i>Pickering v. Board of Education</i> , 391 U.S. 563 (1968)	The Board of Education dismissed a teacher for criticizing the Board’s decision on the distribution of school funds and the superintendent’s explanation as to why additional tax revenues were being sought for the schools.	The U.S. Supreme Court ruled, “The teacher’s interest as a citizen in making public comment must be balanced against the State’s interest in promoting the efficiency of its employees’ public services.” The court held that the teacher’s First Amendment rights were violated when school officials terminated his employment for speaking about a matter of public concern.

TABLE 4. CASE LAW ON THE APPLICATION OF FIRST AMENDMENT PROTECTIONS TO LAW ENFORCEMENT PERSONNEL

<i>Law Enforcement Officers and their First Amendment Right to Free Speech</i>		
<i>Case</i>	<i>Background</i>	<i>Ruling</i>
<i>Locurto v. Guliani</i> , 447 F.3d 159 (2nd Cir. 2006)	A former NYPD officer and two former NYFD firefighters sued Mayor Guliani, Commissioner Safir, Commissioner Von Essen, and the city of New York for illegally firing them from their positions in retaliation for participating in a parade where they mocked stereotypes of African Americans.	The court ruled that “...the defendants fired the plaintiffs out of a reasonable concern for disruption, and that this concern outweighed the plaintiffs’ individual expressive interests...”
<i>Pappas v. Guliani</i> , 290 F.3d 143 (2nd Cir. 2002)	A nonprofit organization sent, via the U.S. Postal Service, a request for donations. In response to this request, an off-duty police officer returned the enclosed envelope but instead of a check he sent racially offensive materials. After an extensive investigation, the NYPD terminated his employment. The officer sued claiming a violation of the First Amendment right.	The court ruled the officer’s dismissal was permissible when the Pickering Test is applied. The officer’s views could impact the effectiveness of the NYPD.
<i>Arndt v. Koby</i> , 309 F.3d 1247 (10th Cir. 2002)	The plaintiff filed suit against the city of Boulder, Colorado, the police chief, and his successor for violations of her First Amendment right to freedom of speech. Detective Arndt was the first officer to arrive at the murder scene of Jon Benet Ramsey. Media publications indicated that the detective and others mishandled the investigation and failed to capture the offender. Because the police chief issued a gag order preventing anyone in the Boulder Police Department from speaking to the media, the detective was unable to defend herself to the press. Furthermore, the chief declined to defend his staff in the press.	Proposed speech is not a matter of public concern, and therefore not protected by the First Amendment.
<i>Lawrenz v. James</i> , 852 F.Supp. 986 (M.D. Fla. 1994)	An off-duty police officer wore a t-shirt with “white power” logo to a private party on Martin Luther King Day. A local newspaper published an article about the police officer, his shirt, and the party. The police officer was terminated.	The court found that the t-shirt was not a matter of public concern and therefore not protected by the First Amendment.

TABLE 4. CASE LAW ON THE APPLICATION OF FIRST AMENDMENT PROTECTIONS TO LAW ENFORCEMENT PERSONNEL (CONTINUED)

<i>Law Enforcement Officers and their First Amendment Right to Free Speech</i>		
<i>Case</i>	<i>Background</i>	<i>Ruling</i>
<i>Flanagan v. Munger</i> , 890 F.2d 1557 (10th Cir. 1989)	Three Colorado Springs police officers equally invested in a video rental store. A fourth investor was responsible for the day-to-day functions of the store. The video rental store made adult films available to adults over the age of 21. Following an investigation, the Colorado Springs Chief of Police “issued written reprimands for violations of sections C 1300 ‘Standards of Conduct,’ C 1301.25 ‘Conduct Unbecoming An Officer,’ and C 1360.01 ‘Obtaining Approval’ for off-duty employment. Chief Munger admitted that plaintiffs would not have been reprimanded for failing to obtain approval for off-duty employment if they had not violated the conduct-unbecoming regulation by renting or selling sexually explicit videos. Thus, it is conceded that plaintiffs’ ‘speech’ activity, renting videos, was the substantial motivating factor of each of the reprimands. The reprimands were placed in each plaintiff’s personnel file.”	The court compared “an employee’s interest in free speech and his employer’s interest in the efficient functioning of government even with nonverbal protected expression.” The court found that the chief of police violated the plaintiffs’ right to freedom of speech.
<i>Berger v. Battaglia</i> , 779 F.2d 992 (4th Cir. 1985)	An off-duty police officer regularly performed in blackface while impersonating the singer Al Jolson.	The court held “that Berger’s conduct in performing public entertainment in blackface was constitutionally protected speech and that the defendants as public employers were not justified by any sufficiently weighty countervailing state interest in taking disciplinary action either punishing Berger for that conduct or chilling in any way his continuation of it.”
<i>McMullen v. Carson</i> , 754 F.2d 936 (11th Cir. 1985)	A clerical employee in the Sheriff’s Office maintained an active membership in the Ku Klux Klan (KKK) and used the media to link himself to the KKK’s activities. The employee was terminated because of the violent nature of the KKK and the racial tension his membership created between the African American community and the Sheriff’s Office.	The court found that the employee’s First Amendment right was not violated and that “...only that a law enforcement agency does not violate the First Amendment by discharging an employee whose active participation in an organization with a history of violent activity, which is antithetical to enforcement of the laws by state officers, has become known to the public and created an understandably adverse public reaction that seriously and dangerously threatens to cripple the ability of the law enforcement agency to perform effectively its public duties.”

discussions ranging from ideology to general rants and raves take place. Figure 5 is a screenshot of a Stormfront forum discussion, located by conducting a search on that website for the phrase “I am a police officer.”

Social Media Guidelines

Social media policies have been instituted by a number of agencies in response to potential liability resulting from employees’ online behaviors. Furthermore cyber postings may reveal sensitive or proprietary information, harass or defame others within the context of the workplace, be threatening or violent in nature, or show disloyalty and insubordination.³¹ For example, in March 2010, three Nebraska correctional officers

were fired for making comments on Facebook about using force against inmates.³² One of the postings stated, “When you work in a prison, a good day is getting to smash an inmate’s face into the ground...for me today was a VERY good day.”

The following social media guidelines may be applied, in whole or in part, to sworn and civilian law enforcement personnel. These guidelines are intended to protect the privacy, confidentiality, and interests of law enforcement agencies and their personnel by clearly describing the types of acceptable and unacceptable cyber behavior and postings.

1. Law enforcement agencies shall notify all personnel when a new cyber-related policy is implemented.

This is Google's cache of <http://www.stormfront.org/forum/archive/index.php/t-255698.html>. It is a snapshot of the page as it appeared on Oct 16, 2009 05:06:12 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

These search terms are highlighted: **i am a police officer** These terms only appear in links pointing to [Text-only version](#)
this page: **stormfront org**

[Stormfront](#) > [Open Forums \(open to guests\)](#) > [General Questions and Comments](#) > Louisiana Police Officer

[PDA](#)

View Full Version : [Louisiana Police Officer](#)

ah

12-18-2005, 01:15 PM

Hey friends~

I am a Police Officer in LOSERana. I am not from the South, and have only been here for a few years. I can't wait to leave!

I am here due to other circumstances, however, I am preparing to go home to the Northwest soon. I took my fiance, who is from Louisiana, back home. The first question she asked was, " where are all the black people?" I explained that there are some, but not alot.

Here in this town (a large city in Northwest Louisiana) it is almost 60% black. There is TWICE as much crime in this city as in my hometown which is 4X as large. I am frustrated every day by the uncivilized behavior of these people. After the hurricanes, alot of that scum from New Orleans came up here and continued thier "behavior of manifested cultural oppression." I think that the Hurricanes just FLUSHED THE TOILET of New Orleans. Now all the TURDS have surfaced in other areas of the country. [Edited by a moderator.]

Anyway, the view from the street is that we are not becoming a more " diverse and tolerant" nation, but one of clear divisions.

John Law

12-18-2005, 01:48 PM

Welcome to Stormfront, ah.

I had to edit your post. Being a police officer I'm sure that you understand why that was necessary. From our Guidelines for Posting:

DO NOT advocate or suggest any activity which is illegal under U.S. law.

FIGURE 5. STORMFRONT POSTING

2. Absent exceptional circumstances, law enforcement personnel may not be prohibited from having a personal website or social networking profile.
 - a. Posting one's affiliation with a law enforcement agency; however, could have an effect on future work assignments (for example, undercover assignments).
3. Law enforcement personnel shall not post, transmit, or otherwise disseminate
 - a. any material that brings discredit to or may adversely affect the efficiency, reputation, or integrity of the agency.
 - b. photographs or depictions of themselves dressed in uniform and/or displaying official identification, patches or badges, trademarks, or logos without prior approval from the chief executive or designee.
 - c. sexual, violent, racial, or ethnically derogatory comments, pictures, artwork, audio, video, or other material on the same website with any online material that references or may negatively affect the public perception of the agency.
 - d. text, pictures, audio, or videos of department training or work-related assignments without written permission from the chief executive or designee.
 - e. sensitive,³³ confidential, proprietary, or classified information to which they have access due to their employment with the agency without prior permission from the chief executive or designee.
 - f. data from criminal or administrative investigations including photographs, videos, or audio recordings without prior permission from the chief executive or designee.

- g. photographs of suspects, arrestees, or evidence, unless it is public information, without prior permission from the chief executive or designee.
 - h. personal statements about a use-of-force incident without prior permission from the chief executive or designee.
 - i. comments related to current or pending prosecutions without prior permission from the chief executive or designee.
 - j. images or details of restricted areas within the facility or its grounds without written permission from the chief executive or designee.
 - k. information about their agency's security procedures without written permission from the chief executive or designee.
 - l. information that could affect the safety or security of the agency or its employees.
 - m. details concerning locations and times of agency activities that are official and sensitive in nature without prior written authorization from the chief executive or designee.
 - n. images or any other materials, obtained during the course of their employment, that reflect the types of sensitive or proprietary technologies used by their agency without prior written authorization from the chief executive or designee.
 - o. comments on the operations of the agency, or specific conduct of supervisors or peers, that might negatively impact the public perception of the agency.
4. Personnel are expected to remain respectful of the agency and its employees, services, partners, and suppliers while blogging or posting in other online venues. Furthermore, employees may not reference agency partners or suppliers in an online forum without express consent of the chief executive or designee.

Additional social media guidelines can be found in the IACP Social Media Model Policy, available at <http://www.IACPsocialmedia.org>.³⁴ It should also be noted that these guidelines must be updated as new mechanisms for online social interaction come into use.

Monitoring

Monitoring law enforcement personnel's cyber postings is an important component of cybervetting. Conducting searches and creating cyber alerts for discussions, posts, videos, blogs, online conversations, and other items that might concern an agency or its personnel will allow that agency to correct false information and rumors and address problematic cyber postings made by employees. The following guidelines provide employees with notice that their cyber behaviors and postings may be viewed by the agency:

1. Law enforcement agencies should periodically inform personnel that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the agency at any time without prior notice.
2. Law enforcement agencies should periodically inform personnel that any information created, transmitted, downloaded, exchanged, or discussed on workplace equipment may be accessed by authorized personnel at any time without prior notice. Workplace equipment remains the property of the agency and no employee has a reasonable expectation of privacy with regard to that information. Agencies may want to document that personnel have received this notice. See Figure 6 for an example of a computer login banner that would allow agencies to document that an employee received proper notification.

Reporting

1. Law enforcement agencies may ask personnel to disclose any website(s) where they have posted information pertaining to their job or employment.
2. Law enforcement personnel who become aware of an Internet posting or website that is in violation of the department's policies shall immediately report that information to a supervisor. See Figure 7. A Photo of a Corpse on Facebook.

The U.S. Department of Defense (DoD) requires the use of a consent banner for desktops, laptops and other mobile devices (DoD, 2008). A user may only access the information system after agreeing to the consent banner (by clicking "OK").

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using or data stored on this IS are not private, and are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (for example, authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

FIGURE 6. EXAMPLE OF LOGIN BANNER

An emergency medical technician (EMT), working for a hospital in Staten Island, New York, was arrested for using his personal camera phone to take a picture of a murder victim.³⁵ The EMT posted the photo on his Facebook profile and a Facebook “friend” reported the photo to the hospital. The hospital terminated the EMT and contacted the New York City Police Department (NYPD).³⁶ The EMT was arrested and charged with official misconduct, a misdemeanor.

The EMT, a retired NYPD detective, pleaded not guilty to the charge and claimed his police instinct led him to take the picture of the crime scene. Furthermore, he claims he inadvertently posted the photo when he uploaded all photos on his camera to Facebook.³⁷ His trial is currently pending.

FIGURE 7. A PHOTO OF A CORPSE ON FACEBOOK

Review of Data

1. When an agency becomes aware of personnel referencing the agency in a personal website, blog, or other online forum, authorized personnel may review the reference to ensure that it does not violate the agency’s policy.
2. In response to concerns or complaints about online postings, the agency may accept, review, and evaluate third party data (for example, a coworker or a concerned citizen).

Social Media Training for Personnel

In the absence of direction, employees will determine for themselves the importance of social media guidelines. In turn, compliance may be inconsistent. Educating employees on the purpose of social media guidelines and the intent behind them will increase understanding and cooperation, and reduce risk associated with employees’ cyber postings. The following guidelines should be considered for incorporation into cyber training designed to teach employees responsible web behaviors:

1. Personnel should be notified that the department’s standards of behavior, including harassment and anti-disparagement policies, apply to online behavior.

Table 5 presents the case of *Blakey v. Continental Airlines* (2000), a sexual harassment case from the 1990s. This case is unique in that it was the first to address coworker harassment in cyberspace. Furthermore, “... the *Blakey* decision demonstrates the potential for employer liability in situations where employee blogging goes unmonitored. Although the case provides

little guidance on where an employer should draw the line in monitoring activity, it demonstrates that the potential for liability exists.”³⁸

2. Law enforcement agencies should educate personnel on what constitutes an appropriate web presence as it relates to representing their agency and personal safety. Briefings should include but are not limited to
 - a. copyright, trademark, and other intellectual property laws and how they affect what employees can post online;
 - b. the impact that Internet postings and other electronic communications have on people’s ability to work in assigned positions (for example, undercover assignments), and active criminal cases (for example, impeached testimony);
 - c. the fact that personal and work-related information posted by employees, their families, or their friends may be misused; and

Reputation and Safety

Search engines are powerful tools in the hands of law enforcement, but officers should be reminded to protect their online reputations and stay aware of what can be found about almost anyone on the Internet from social networking sites and other databases. For more information on personal safety, visit DoD’s *Social Media Hub, Education and Training* @ <http://socialmedia.defense.gov>.

TABLE 5. CASE LAW PERTAINING TO COWORKER HARASSMENT IN CYBERSPACE

Case	Background	Ruling
<i>Blakey v. Continental Airlines</i> , 751 A. 2d 538 - NJ: Supreme Court 2000	A female pilot sued her employer, Continental Airlines, for sexual harassment and a hostile work environment. In 1995, several Continental pilots published “harassing gender-based messages” to an electronic bulletin board called the <i>Crew Members Forum</i> . This electronic bulletin board was located on a Continental website used by crew members to learn their work schedules. However, in order to access the <i>Crew Members Forum</i> , crew members had to pay a monthly fee to CompuServe, the Internet service provider.	The Supreme Court of New Jersey found that “harassment by a supervisor that takes place outside of the workplace can be actionable... employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop coemployee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace.”

During the summer of 2009 the following post appeared on the Massachusetts Law Enforcement Network:

Threat to a Police Officer on FACEBOOK.....

I recently had the opportunity of receiving a THREAT from an anonymous person (fake name, shocker!). It is now under police investigation, but I just had a few questions.....(1) has anyone here had any luck with getting info from FACEBOOK during a criminal invest? (2) do you think the Detective(s) assigned will be able to pinpoint what computer (who owns a cpu, etc.) it came from after speaking with FACEBOOK (I got the threat in a Facebook e-mail via the INBOX)? Any other info is appreciated. I hope to be able to find out the identity of the person who has made a pretty detailed threat to me.....

PS: The only thing they could get off of me on FACEBOOK was my name because I have all of the security measures in place etc. The disturbing part is how they seemed to know a lot of details anyways about me. Probably someone I arrested, who knows..... again, anything that could help in the invest would be greatly appreciated. Thx

FIGURE 8. CYBER THREATS

- d. privacy settings at social media sites are constantly in flux. One should never assume that personal information posted at these sites is protected.

Figure 8 is a posting made by a police officer who was threatened via Facebook and who also believed his personal information was protected on Facebook.

Authentication

This section addresses the assessment of the validity and reliability of online information pertaining to applicants, candidates, and incumbents. The Internet is an evolving resource for background investigations. Search engines help investigators identify sources of information concerning a specific person but almost anyone can create a website or post online content, and this accessibility impairs one’s ability to recognize records of fact from opinion and sometimes even fiction. For example, an investigator may be able to establish

that an existing Facebook profile matches the name and appearance of a subject, but how can an investigator know for sure, without consulting the subject or subpoenaing the service provider, if the Facebook profile was created by the subject? See Figure 9 for a real-life example of a fraudulent Facebook profile and Figure 10 for information on how to report a fraudulent social networking account.

Policy

Given (1) it is often difficult to know with certainty that information obtained from public areas on the Internet pertains to the actual person of interest, (2) people can maliciously place false information about people on the Internet, and (3) unintentional errors at certain public sites on the Internet are common, law enforcement agencies should attempt to verify information collected from the Internet is accurate and truly associated with the person of interest.

In 2009, a Carmel, California, high school teacher discovered that someone created a Facebook profile in his name. The profile creator used the teacher’s name and date of birth to create a fictitious Yahoo e-mail account and then used the teacher’s yearbook photo and fake e-mail address to establish the Facebook account.

The teacher became aware of the Facebook account only after a student, “friended” by the phony Facebook teacher, complained to the school’s administration that the teacher was harassing him. Later, the teacher realized that at least six other students had also been harassed.

The FBI and U.S. Attorney’s Office were notified and immediately began investigating the case as a possible violation of the Computer Fraud and Abuse Act. In addition, the teacher filed suit against unidentified individuals claiming defamation, intentional and negligent infliction of emotional distress and fraud.³⁹ The teacher’s attorney served civil subpoenas to Yahoo and Facebook in an effort to obtain the IP address of the computer on which the bogus accounts were created.⁴⁰

The fraudster was eventually identified and the lawsuit settled out of court. The amount of the settlement and the defendant’s name were not disclosed. The money received from the settlement was donated to a nonprofit organization that provides assistance to teachers victimized by this type of fraud.⁴¹

FIGURE 9. FRAUDULENT SOCIAL MEDIA PROFILE

Facebook

“If someone has created an account to impersonate or imitate you, go to the imposter profile and click ‘Report this Person’ in the left column. Check the ‘Report this Person’ box, choose ‘Fake Account’ as the reason, and add ‘impersonating me or someone else’ as the report type. Be sure to add a valid Web address (URL) leading to the real profile to that we can review the information.”⁴²

LinkedIn

“Contact Customer Service through the link at the bottom of your home page to report an inappropriate profile. In your message, please include the full name on the profile and a link to the page where it appeared. The LinkedIn Privacy group will review the profile and take appropriate actions based on our findings (retrieved on June 15, 2010).”

Twitter

“In order to investigate impersonation, we need the following information:

- Username of the person impersonating you (or the URL of their profile page):
- Your first and last Name:
- Your Twitter username (if you have one):
- Address:
- Phone:
- Brief description of the impersonating content:

If you are not the person involved in the impersonation, but are legally authorized to act their behalf, please include the information above in addition this information:

- Your name:
- Phone:
- Fax:
- Company website:
- Company domain e-mail address:
- Your title and legal relationship to the person/entity involved:

How do I report an impersonation violation?

To report an impersonation, please submit a ticket request with the information requested above. Be sure to select *impersonation* from the drop-down menu. If you submit while logged into your Twitter account, you’ll be able to check on your ticket status anytime by visiting your Twitter Support home page and clicking on *check on your existing requests*.

If you don’t have a Twitter account or are unable to log in to reach the form, please also visit the ticket request form and click the blue *No account? Login problems?* link in the lower right. Once you’ve submitted your ticket, we’ll e-mail you a ticket confirmation with more information.”

FIGURE 10. REPORTING FRAUDULENT SOCIAL NETWORKING ACCOUNTS

Practices

The development of authentication practices should take into consideration malicious cyber postings, fraudulent social networking profiles, and the number of ways cybervetters can introduce error into the results. For example, using a subject’s name as a search term may yield several thousand results, especially if it is a common name. Information pertaining to that subject may be discarded by the person conducting the search because of the possibility that the information belongs to someone else with the same name. On the other hand, searchers may assume that all online information pertaining to a subject with an uncommon name is related to that subject.⁴³

Another issue of concern is the compromise of social networking accounts.⁴⁴ Increasingly, social network users’ profiles and pages are compromised either through user error, social engineering,

phishing, or software flaws. Providing applicants, candidates, and incumbents with the opportunity to refute online content associated with them should minimize the risk of rejecting a suitable applicant or candidate, or disciplining an incumbent for online actions that were beyond their control. Indicators of a compromised social networking account are provided in Figure 11.

The following guidelines are provided in an effort to minimize the impact of malicious postings, fraudulent social networking profiles, and search-related errors:

1. Law enforcement agencies should ask applicants, candidates, and incumbents to confirm the accuracy of any information found online. Applicants, candidates, and incumbents should be allowed to provide the names of references who can speak knowledgeably about the online information of concern.

Any unexpected changes to a social networking profile may indicate a compromised account. Some changes to look for include:

- A significant change in the number of friends
- Modifications to wall posts and pictures
- Applications added to the profile
- The design of the profile was altered
- The password no longer works
- An e-mail is received from the social networking site stating that changes have been made to your profile
- The profile reflects changes to identifying information
- The profile shows unfamiliar group memberships

FIGURE 11. INDICATORS OF A COMPROMISED SOCIAL NETWORKING PROFILE

2. Law enforcement agencies may provide a copy of online data used to make employment decisions to any individual who was the subject of the agency's cybervetting procedures and who makes a request for their information.
3. Law enforcement agencies should recommend that candidates and incumbents correct erroneous information about them posted on the Internet.

Adjudication

Employees, both public and private, have been fired, disciplined, or eliminated from consideration for employment because of the information they posted or statements they made online.⁴⁵ The

following section addresses the incorporation of cyber data into the decision-making process for law enforcement as well as the impact it may have on hiring, retention, promotion, and disciplinary decisions. See Figure 12 for information concerning a police officer who was disciplined for online comments made in reaction to a news article.

Table 6 reflects case law pertaining to a disciplinary decision concerning a police officer's cyber postings. The police officer was fired and he appealed the decision, claiming employment termination was a severe penalty and not consistent with his behavior. Both the trial court and the court of appeals found in favor of the City Council's decision to dismiss the officer.

In May 2010, the Columbia, Missouri, SWAT team raided a home looking for marijuana. During the course of that raid, one pit bull was killed and another dog badly injured. In response, the community organized a protest at the local post office.⁴⁶ While attending the protest, a local newspaper captured a photo of a subject holding a sign that said "Stop Brutality." The story of the protest, including the subject's image and quote, were included on the newspaper's website.

A reader posted on the newspaper's online comments section:

Seeing the people of Columbia stand up to this totally unacceptable police brutality refreshes my pride in America.

A police officer and member of the Columbia SWAT team responded to that post with the following:

The guy with the 'stop the brutality' sign has multiple convictions for assaulting people with guns!!! I'd like him to stop the brutality of humans!

Another reader posted:

[name Redacted] in the picture, can file a defamation of character and slander against you ... so maybe a retraction should be in order.

The officer responded:

It ain't slander if it's true. It is.

After a 6-week investigation, the police department determined that the officer violated his duty to safeguard information. The officer received 120 hours without pay.⁴⁷

FIGURE 12. POSTING SENSITIVE INFORMATION ON THE INTERNET

TABLE 6. CASE LAW CONCERNING ONLINE BEHAVIOR

Case	Background	Ruling
<p><i>Cromer v. Lexington-Fayette Urban Co. Govt.</i>, #20088-CA-000698, 2009 Ky. App.</p>	<p>A Lexington, Kentucky, police officer arrested singer John Michael Montgomery for DUI. The publicity from this arrest increased the number of visitors to the officer’s MySpace page. The City Council found that “on or about March 20, 2006, Officer Cromer, identifying himself as a Lexington Police Officer through word and image, posted, or allowed to remain posted, to website MySpace.com language and/or images that reflected discredit upon Officer Cromer as a member of the Division of Police, brought the Division into disrepute, and impaired the operation and efficiency of himself and the Division. Such postings include profane language; inappropriate or derogatory comments or images concerning homosexuals and the mentally disabled; inappropriate or derogatory comments about the people and/or the city of Lexington; inappropriate comments concerning the use of force; an entry concerning the use of his authority for his own benefit related to a car alarm that was annoying him; the use of his authority for the benefit of a friend by not arresting the friend for DUI; inappropriate sexual comments; and an altered photograph depicting him with John Michael Montgomery after he had arrested Mr. Montgomery for DUI.” The officer’s employment was terminated by the City Council.</p>	<p>Both the trial court and court of appeals affirmed the City Council’s decision to terminate employment for misconduct, inefficiency, and insubordination.</p>

Hiring, Retention, Promotion, and Disciplinary Decisions

Law enforcement agencies should already have hiring, retention, promotion, and disciplinary policies and practices in place. This section of the guidelines serves as a reminder that authenticated online information should be used to make employment decisions the same way information from any other source would be used. However, agencies that make adverse employment decisions using online information provided by a consumer reporting agency (that is, a third party) will need to meet the requirements established by the FCRA. See Figure 13.

1. Hiring, retention, promotion, and disciplinary decisions may be affected by information found on the Internet.
2. Hiring, retention, promotion, and disciplinary decisions must be based on established criteria and processes. See Figure 14.
3. Information, regardless of the source, should only be considered when it falls within the scope of the investigation, unless out-of-scope information reflects behaviors that could impact the ability of the applicant, candidate, or incumbent to perform his or her duties.

Incumbents

1. Law enforcement personnel
 - a. whose actions can be directly linked to websites that promote misconduct or bring discredit to the agency or a member of the agency, unless linked for official work-related purposes, should be investigated.
 - b. who violate their agency’s social media policies shall be appropriately disciplined by the chief executive or designee.

Out-of-Scope Behavior

During the focus groups, some law enforcement executives expressed concern about reviewing and adjudicating evidence, located online, of disqualifying behaviors that fall outside the scope of the background investigation.

Adverse employment decisions based on information from third parties are governed by the FCRA. Law enforcement agencies using third parties for cybervetting purposes will need to provide (1) notice of disciplinary action, (2) contact information of the third party, (3) assertion that the third party played no role in the employment decision and cannot provide information as to how the decision was reached, and (4) notice that the affected party may request a free copy of the report along with an explanation as to how the employer reached its decision.⁴⁸

FIGURE 13. ADVERSE EMPLOYMENT DECISIONS AND THE FCRA

A former Delta Airlines flight attendant claimed she was fired for posting images of herself in uniform on her blog. She argued that her termination constituted sex discrimination because Delta did not discipline male flight attendants for similar postings.

The flight attendant filed a claim with the Equal Employment Opportunity Commission against Delta. Delta filed for bankruptcy shortly after the claim was filed and the case has still not been heard in court.

See *Simonetti v. Delta Airlines Inc.*, No. 5-cv-2321 (2005).

FIGURE 14. EQUAL TREATMENT

Training

Law enforcement agencies should already have existing policies and practices concerning the evaluation of information used to make employment decisions. Online information is more complex because technology is constantly evolving and almost anyone can create or modify online profiles, blogs, and other online content. Decision makers are responsible for ensuring that employment decisions are based on accurate and complete information.

Therefore, the following training item is suggested:

1. Law enforcement agencies shall ensure decision makers are properly trained on evaluating cyber search results.

Safeguarding Data

A sound data protection plan is essential when agencies maintain personal information found on the Internet, even if that information was not protected by a password. Intentional or accidental disclosure of personal information may cause the person affected to feel embarrassed, or in more serious situations lead to fraud or identity theft. Failure to protect personal information may expose an agency to civil suits.

The following guidelines will help agencies properly protect information collected during the cybervetting process:

1. When collecting data, employers must consider the responsibilities associated with data collection, retention, and storage.
2. Cybervetting results should be safeguarded in a manner that is consistent with existing Human Resource policies and practices pertaining to employment and background investigation data.
3. The retention of cybervetting results should comply with existing document retention policies.
4. Law enforcement agencies should address the unauthorized disclosure of information obtained from the cybervetting process.
 - a. A process should be in place to inform applicants, candidates, and incumbents if their cybervetting results have been inappropriately disclosed.
 - b. Unauthorized disclosure should result in disciplinary action.

SECTION 3. ADDITIONAL RESOURCES

The following list of books and websites pertaining to cybervetting and social media is not exhaustive. These resources are provided as a starting point for any agency that plans to develop cybervetting and social media strategies.

A. Cybervetting

Grant Harpe, Lisa D., *Social Networks and Employment Law: Are You Putting Your Organization at Risk?* People Click, 2009. http://www.peopleclick.com/resources/wpaper/Social_Networks_Employment_Law_eBook.pdf (accessed October 8, 2010).

Lee, David and Shane Witnov, *Handbook on Conducting Research on Social-Networking Websites in California*, http://www.law.berkeley.edu/files/Social_Networking_Website_Research-Handbook.pdf (accessed October 8, 2010).

Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age*. Princeton N.J.: Princeton University Press, 2009. <http://press.princeton.edu/titles/8981.html> (accessed October 8, 2010).

B. Social Media

Boudreaux, Chris, "Social Media Governance." 2009–2010, <http://socialmediagovernance.com/policies.php> (accessed October 8, 2010).

Department of Defense, "Welcome to the Social Media Hub," <http://socialmedia.defense.gov/> (accessed October 8, 2010).

Intel, "Intel Social Media Guidelines," http://www.intel.com/sites/sitewide/en_US/social-media.htm (accessed October 8, 2010).

International Association of Chiefs of Police, "Center for Social Media," <http://www.IACPsocialmedia.org>.

Lauby, Sharlyn, "10 Must haves for Your Social Media Policy," Mashable.com, June 2, 2009. <http://mashable.com/2009/06/02/social-media-policy-musts/> (accessed October 8, 2010).

"Reporting from the Internet," *Handbook of Journalism*, Thomson Reuters, 2010. http://handbook.reuters.com/index.php/Reporting_from_the_internet (accessed October 8, 2010).

Schweitzer, Tamara, "Do you need a Social Media Policy?" *Inc.*, January 25, 2010. <http://www.inc.com/articles/2010/01/need-a-social-media-policy.html> (accessed October 8, 2010).

C. Internet Safety

Federal Trade Commission, "On Guard Online," n.d., <http://www.onguardonline.gov/> (accessed October 8, 2010).

Privacy Rights Clearinghouse, "Online Privacy: Using the Internet Safely," <http://www.privacyrights.org/fs/fs18-cyb.htm> (accessed October 8, 2010).

Wired Kids, Inc., "Wired Safety," <http://www.wiredsafety.org/> (accessed October 8, 2010).

D. Privacy

American Civil Liberties Union, "Internet Privacy," <http://www.aclu.org/technology-and-liberty/Internet-privacy> (accessed October 8, 2010).

Electronic Frontier Foundation, <http://www.eff.org> (accessed October 8, 2010).

Electronic Privacy Information Center, "Social Networking Privacy," <http://epic.org/privacy/socialnet/default.html> (accessed October 8, 2010).

European Union, – *Data Protection Directive 95/46/EC*, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (accessed October 8, 2010).

Federal Trade Commission, Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., www.ftc.gov/os/statutes/031224fcra.pdf (accessed October 8, 2010).

SECTION 4. ACKNOWLEDGEMENTS⁴⁹

A. IACP's Private Sector Liaison Committee

Committee Co-Chair
Special Agent in Charge Rad Jones (Retired)

Committee Co-Chair
Commissioner Rocco Diina (Retired)

B. IACP's Professional Standards, Image, and Ethics Committee

Committee Chair
Chief Ronald McBride (Retired)

Staff Liaison
Charlie Higginbotham

C. IACP's Computer Crime and Digital Evidence Committee

Committee Chair
James Emerson

Staff Liaison
David Roberts

D. IACP's Psychological Services Section

Section Chair
Phillip Trompetter, Ph.D.

Staff Liaison
Kim Kohlhepp

E. Focus Group Hosts⁵⁰

The following people and organizations deserve special recognition for hosting a focus group:

Monterey, CA

Defense Personnel Security Research Center

Plano, TX

Daniel P. Carlson
Institute for Law Enforcement Administration

St. Paul, MN

Tim Thompson
Verifications, Inc.
Marie Ohman
Minnesota Private Detective & Protective Agent Services Board

Chicago, IL

Susan Korin
Michael R. Stowers
Stephen Griffin, Psy.D.
Institute for Personality and Ability Testing, Inc.

Denver, CO

Lieutenant Matthew Murray
Denver, CO, Police Department

Plano, TX

Chief Ronald McBride (Retired)
International Association of Chiefs of Police
Professional Standards, Image, and Ethics Committee

Atlanta, GA

Chief Terry Sult
Sandy Springs, GA, Police Department
Chief Joe Estey (Retired)
iXP Corporation

Orlando, FL

Carrie Whitcomb
National Center for Forensic Science

Redmond, WA

Computer Forensic Investigator Jan Fuller
Lieutenant Charlie Gorman
Redmond, WA, Police Department

Baltimore, MD

Chief Mike Gambrill (Retired)
Dunbar Armored, Inc.
Chief David Crawford
Laurel, MD, Police Department
Steve Somers
Allied Barton Security

Falls Church, VA

Ray Musser
Rosalind Baybutt
General Dynamics

Akron, OH

Dennis Doverspike, Ph.D.
University of Akron

Wayne, NJ

Cynthia Hetherington
Hetherington Group

Boston, MA

Agnes Chan, Ph.D.
Northeastern University

Toronto, Canada

Superintendent Dave Truax
Ontario Provincial Police

F. Focus Group Participants

The following people contributed their time and expertise to this effort:

Monterey, CA

Chief Louis Fetherolf
Simson Garfinkel, Ph.D.
Joanie Gillispie, Ph.D.
William Henderson
Helgi Jonsson
Theresa Merry
Shane Witnov

Plano, TX

Commander Luis Almaguer
Lieutenant Steven Baxter
Lieutenant John Bennett
Lieutenant Ben Brown
Sergeant James Bunger
Lieutenant Chris Butterworth
Sergeant Kevin Campbell
Lieutenant Michael Dotson
Lieutenant James Foust
Lieutenant Eddie Garth
Lieutenant Scott W. Haynes
Sergeant Sherwood E. Holmes
Sergeant Jon “JP” Jacob
Lieutenant Gene Kropff
Lieutenant Alex Lopez
Sergeant Jason McCaffity
Lieutenant Frank Medrano, III
Sergeant Randy Meyer
Lieutenant Doug Mitchell
Deputy Mitchell Morgan
Sergeant John Mutchler
Lieutenant Dennis Norton
Lieutenant Gregory Oballe
Lieutenant Garland G. Payne
Lieutenant Jeffrey D. Pugh
Lieutenant Gerald Quiat
Sergeant David Rodriguez
Captain John Rodriguez
Lieutenant Mike Sharp
Chief Jeffery “Jake” Sullivan
Lieutenant John Voss
Lieutenant Raymond Williams

St. Paul, MN

Michael Brewer
Chief Jim Franklin (Retired)
Chris Gustafson
Rick Hodsdon, Esq.
John Kaul, Esq.
Steven Klein
Sergeant Paul Lenzmeier
Paul Luehr
Bob Meissner

Director Neil Melton
Clay Narum
Ann O’Brien
Lori Olson
Desyl Peterson, Esq.
Mary Poquette
John Weaver

Chicago, IL

Eve Gohoure
Laura Kunard, Ph.D.
Leslie Ann Reis, Esq.
Wayne Schmidt, Esq.
Chief Thomas Sheahan
Mike Crane, Esq.
Dan Shoemaker

Denver, CO

Sara Garrido
Officer Eric A. Gonzales
Earl E. Peterson
Don Ronyak
Antoinette Torres-Janke

Plano, TX

Special Agent in Charge Glenn Anderson
Chief Gregory J. Anderson
Chief Steven Annibali
Chief Ronnie Bastin
Chief Chuck Bennett (Retired)
Daniel P. Carlson
Chief John H. Cease (Retired)
Assistant Commissioner Pat Cummins (Retired)
Jeff G. Fackler
Chief Michael Force
Special Agent in Charge Robert D. Grant
Charles Higginbotham*
Chief Steve Martin
Tom Martinelli, Esq.
Phyllis P. McDonald, Ph.D.
Secretary Walter A. McNeil
Chief Richard Melton
Chief Ronald L. Miller
Executive Assistant Chief Martha Montalvo
Robert Neff
Captain Mark O’Toole
Patricia Robinson, Ph.D.
Chief Lynn S. Rowe (Retired)
Wayne Schmidt, Esq.
Chief John G. Simmons
Chief Gary Smith
Chief John Young
Alan C. Youngs, Esq.
Chief Garrett W. Zimmon (Retired)

*IACP staff

Atlanta, GA

Butch Beach
Chief Stacey L. Cotton
Philip Davis
Chief Lou Dekmar
Chief Joe Estey (Retired)
Chief Dan Flynn
Chief Billy Grogan
Sergeant Shad Hutchins
Sergeant Ronald L. Momon Jr.
David Poston, Esq.
Anthony Ritter
Assistant Chief Constable Gordon Scobbie
Lauri Stevens
Police Cadet Paul Walkin
Supervisory Special Agent David A. West
Lieutenant Gina V. Yabuku

Orlando, FL

Chief Bill Berger
Assistant Director Dave Heffernan
Director Jeffrey Goltz
Assistant IG Sam Guttman (Retired)
Lieutenant Sue Manney
Chief Brett Railey
Bobbi Willoughby

Redmond, WA

Valerie Bunn
Francis D'Addario
Chief Ron Gibson
Virginia Gleason
Chief Steve Harris (Retired)
Jeffrey McCall, Ph.D.
Commander Terry Morgan
Chief Don Pierce (Retired)

Baltimore, MD

Sergeant Robert Alexander
Lieutenant Pat Bray
Major Joseph Burris
Sally Burt
Jon Cano
Jim Christy
Lieutenant Edward Johnson
Colonel George Johnson
Captain Luther Johnson
Corporal Gary Kulik (Retired)
Al Liebno
Sergeant Erik Lynn
Sergeant Bryant D. Moore
Stephen Prozeralik
Assistant Special Agent in Charge Adam D. Schneider
Major Michael G. Sewell
Stephen Shaver
Mark Sheppard
Lieutenant John Superson

Peter J. Tollini
Chris Wargo
Amy Youngman

Falls Church, VA

Sandra Barksdale
Kym Baum, Ph.D.
Robby Ann Carter
Bryan Castelda, Ph.D.
John Creswell
Patrick Donahue
Rob Doolittle
Joe Downey
Tara Dunlap
Richard "Lee" Engel
Al Hein
Rick Hohman
Matthew Hollandsworth
Vincent Jarvie
Marc Jenkins
Matthew Lancaster
Tom Langer
Peter Nelson
Barbara Petitti
Danielle Whitfield
Quinton Wilkes

Akron, OH

Lawrence Borodkin
Dennis Byrne
José A. Caraballo
William D. Evans II
Jeff Gross
Cathy Hanlin
Donald M. Jenkins
Chief Michael B. McNeely
A.G. Monaco
Elayne Siegfried, Esq.
Teresa Thompson
Beth Tritica
Jaime Umerly, Esq.
Tara Weber
Kelly Zachary

Wayne, NJ

Christopher M. Arunkumar
Steven Branigan
Dorian Buckethal
Captain James J. Clarke
Allison Cunningham
Brian DeFelice
James J. Emerson
Keyana C. Laws, Esq.
Heather McDade
Dana Marsalisi
Bill Majeski
Robert O'Leary

Elizabeth Rincon
Officer Joe Rude
Maurizio P. Scrofani
Pete Staats
Keith Talbert
Jason Thomas
George Wade

Boston, MA

Lisa Bernt
Richard M. Feustel
Thomas Koenig
Alan Mislove
Gregory Moore
Captain Mark O'Toole
Themis A. Papageorge
Bhavesh Patel
David Papargiris
Lauri Stevens

Toronto, Canada

Zachariah Ezekiel
Philip Fisher
Lisa Henderson
Dennis Herdman
Ed Jarosz
Rowena Kenny

Kurt Kreuger
Lorraine Leung
Denis McBride
Detective Sergeant Shawn Nash
Constable John Rozich
Bjorn Rutten
Mark Saltmarsh
Detective Sergeant Kim Scanlan
Shelley Sweeney
Sandy Thomas
Joseph Versace

Alexandria, VA

Chief David Crawford
Dennis Doverspike, Ph.D.
Chief Joe Estey (Retired)
Chief Mike Gambrell (Retired)
Chief Michael Force
Ben Gorban*
Stephen Griffin, Psy.D.
Chief Mark Marshall
Rebecca McClelland*
Dan Primozic, Ph.D.
Stephan Somers
Mike Stowers
Chief Terry Sult

G. Survey Respondents

The following people provided feedback to the initial set of policies and practices culled from the literature review and SME interviews.

Sergeant Tim Albright
Christina Keibler Bolas
Lynn Bowler
David A. Bray
Chief Randall Carroll (Retired)
Chief John Cease (Retired)
Sally Cunningham
George M. Dery III
Stephan Dilchert, Ph.D.
Dennis Doverspike, Ph.D.
Nicole Ellison, Ph.D.
James J. Emerson
Tiffany Ford
Jan Fuller
Chief Dan Flynn
Sergeant Scott French
Simson Garfinkel, Ph.D.
Joanie Gillispie, Ph.D.
Samuel D. Gosling, Ph.D.
Cynthia Hetherington
Lieutenant Wayne Kitade
Steven M. Kleinman
Chief Ronald W. McBride (Retired)
Robert Morgester
Cassandra Murphy

Inspector Rod Nakanishi
Peter Nelson
Captain Noblett
Jennifer O'Connor, Ph.D.
Deniz Ones, Ph.D.
Steve Otto
Captain Kenneth (Nate) Phillips
Jone Papionchock, Ph.D.
Mark M. Pollitt
Karla Porter
Commander Steve Potter
Commander Craig Potter
Captain Risedorph
Joel R. Reidenberg, Ph.D.
Peter A. Rosen, Ph.D.
Jane Sachs
Sergeant Dan Schnepple
Sergeant Jeff Scott
Jarrett Shalhoop, Ph.D.
Michael Stowers
Professor Robert Sprague
Kevin Tamanini, Ph.D.
Detective Liam Walker
Shane Witnov
Sergeant Joe Young

*IACP staff

H. Additional Contributors

This project benefited greatly from discussions with the following scholars and practitioners:

Chief R. Steven Bailey
Miami Township Police Department

Donna Braxton
Executive Director
Ohio Association of Chiefs of Police

Simson Garfinkel, Ph.D.
Naval Postgraduate School
Center for Information Systems Security Studies and
Research

William Herbert, Esq.
New York State Public Employment Relations Board

Joel Reidenberg, Ph.D.
Fordham University School of Law

Professor Paul Schwartz
University of California, Berkeley School of Law

Scott R. Shipman
Associate General Counsel
eBay Inc.

SECTION 5. GLOSSARY

Adjudication: a determination based on an assessment of an individual's loyalty, reliability, trustworthiness, and fitness for a responsibility.

Applicant: individuals applying for employment.

Authentication: the process of establishing facts or evidence thereof, such as obtaining corroboration from different sources or determining direct authorship of a document.

Blog: a self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."

Blogger: a blogging platform also known as a Blogspot; someone who blogs.

Candidate: a job applicant who is under consideration for a job offer.

Consent: permission to proceed with what is planned or done by others; documented acceptance by an individual of certain specified conditions.

Copyright: the legal right granted to an author, composer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.

Cyber alerts: e-mail updates of the latest relevant search engine results on a specified topic.

Cyber behavior: see online behavior.

Cyber bullying: willful and repeated harm inflicted through the use of electronic communication devices.

- there is a pattern of behavior
- the target feels hurt or humiliated

Cybervetting: an assessment of a person's suitability to hold a position or security clearance using in part information found on the Internet.

Due process: providing an employee with notice of an adverse employment decision, the opportunity to respond to the decision, and the right to appeal any final decision.

E-mail: short for electronic mail; a method of exchanging messages over the Internet or intranet.

Employee: a person who works for another in return for financial or other compensation.

Employment decision: any decision that affects offers of employment, or the terms or conditions of employment (e.g., hiring, transfers, promotion, demotion, termination).

Facebook: a social network site that allows users to create profiles, send messages, create networks of friends and fans, and share content.

Fair Credit Reporting Act (FCRA): 15 U.S.C. § 1681, regulates the collection, dissemination, and use of consumer information, including consumer credit information.

Follower: on Twitter, a person who subscribes to receive tweets from a registered user.

Friend: an individual who is part of another individual's network.

Friend request: the act of requesting someone to be your friend on Facebook, in which they can accept or reject you. If they accept, you become a part of their network and they become a part of your network.

Example 1: I'm "friending" Lisa on Facebook right now, I hope she accepts!

Example 2: Oh, I'm going to "friend" her too!

Identity theft: a catch-all term for crimes involving illegal use of another individual's identity.

Internet (also the World Wide Web, or the Web): A global system of interconnected computer networks that host a variety of applications that allow users to communicate and interact with each other.

Internet searches/cyber searches: a process of locating and retrieving data (written documents and other media such as images, video and audio files) available on the Internet.

LinkedIn: a social network site focused on professional network connections

Metasearch engines: a metasearch engine submits queries to multiple search engines and returns an aggregate result of multiple searches.

Metasearches: Internet searches conducted on metasearch engines.

Microblog: service that allows users to send short (usually character restricted) messages out to a network of followers; examples include Twitter and Nixle.

Monitoring: the continuous conduct of cyber or Internet searches for any discussions, posts, videos, blogs, online conversations, etc., of your department with the purpose of discovering what is being said about you and being able to correct false information or rumors.

MySpace: a social network site.

National security positions: (1) Those positions that involve activities of the government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and

(2) Positions that require regular use of, or access to, classified information. Procedures and guidance provided in OPM issuances apply.

(3) The requirements of this part apply to competitive service positions and to Senior Executive Service positions filled by career appointment within the Executive Branch, and agencies may apply them to excepted service positions within the Executive Branch.

Notice: documented communication to an individual of specified conditions.

Online behaviors: broadly includes all activities using computer technology, including the transmission of information, completion of tasks, replication of noncomputer activities, and creation of novel activities.

Replication of noncomputer activities: Some cyber activities are easily described and understood, for technology merely provides a more efficient way of doing common things. These include using e-mail instead of phone conversations or postal mail, looking up information on the web instead of using an encyclopedia or a telephone book, and interacting with people via social networking and microblogging websites such as Facebook and Twitter instead of talking to them in person.

Creation of novel activities: In contrast to those cyber environments that replicate real world activities, some create novel activities with a strong resemblance to real world places, people, and things, but that also go wildly beyond real life and into imagination. The most well known examples are: Grand Theft Auto, Doom, The Sims, World of Warcraft, and Second Life.

Online profile: a description of a user of a network. The description can include biographical data, pictures, likes, dislikes, and any other information a user chooses to post.

Page: The specific portion of a social media website where content is displayed and managed by an individual or individuals with administrator rights.

Post: Content an individual shares on a social media site or the act of publishing content on a site.

Preemployment screening: the manner in which organizations proactively examine potential employees, including contractors, subcontractors, and temporary hires, for personal and professional history and characteristics related to their qualifications, fit, and risks as employees.

Privacy settings: an option many social media sites offer to allow a user to determine the level to which their information is made available to others.

Profile: information that users provide about themselves on a social networking site.

Sensitive position: (1) positions that are directly responsible for the health, safety, and welfare of the general population or the protection of critical infrastructures; or (2) any position so designated within an organization, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the organization or national security.

Social media: a category of websites that is based on user participation and user-generated content. They include social networking sites like LinkedIn, Facebook, or MySpace, microblogging sites like Twitter, social bookmarking sites like Del.icio.us, social news sites like Digg or Reddit, and other sites that are centered on user interaction.

Social media policy: guidelines that pertain to employees' interaction with social media websites. Employees are often encouraged to follow these guidelines but in some cases employees are required to follow the guidelines or risk disciplinary action.

Social networking sites: online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

Speech: expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Twitter: a microblogging tool that allows users to send short messages (up to 140 characters) that will immediately be distributed to their network of followers.

Upload: to transfer data from a personal computer or device to a larger entity such as a website.

Visual search engine: a search engine that looks for information on the World Wide Web through the input of an image.

Web 2.0: the second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.

Web page: a multimedia document (may contain text, images, audio, and/or video) that is accessible on the Internet. A web page may be static (a user only views) or interactive (a user may input data and alter the content). Web pages often have links that direct users to other web pages.

Web presence: any information available on the Internet about an individual which is also under the control of that individual.

Website: a collection of interlinked web pages which are generally authored, hosted, and maintained by a single entity. Websites are commonly used to represent entities such as government organizations, businesses or persons, or used as places for individuals with common interests to meet and interact.

SECTION 6. NOTES AND CITATIONS

The following references are cited within the text of the report:

¹Approximately 80 percent of Americans have a computer in their home, and roughly 92 percent of those people have an Internet connection. Nearly 60 percent of adult Americans use wireless Internet. Cell phones have also increased access to and the amount of content found on the Internet. Forty percent of adult cell phone owners use their phones to access the Internet, e-mail, or instant messaging; 76 percent take pictures with their phones; and 34 percent have recorded a video with their phone. Nielsen//NetRatings, “Home Internet Access in U.S.: Still Room for Growth,” March 11, 2009, <http://www.marketingcharts.com/interactive/home-Internet-access-in-us-still-room-for-growth-8280/> (accessed July 7, 2010); and Smith, Aaron, *Mobile Access 2010*, Pew Internet and American Life Project, July 7, 2010. <http://pewInternet.org/Reports/2010/Mobile-Access-2010.aspx?r=1> (accessed August 9, 2010).

²Jaksic, Vesna, “Finding Treasures for Cases on Facebook,” *The National Law Journal*, October 15, 2007, <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1192179809126> (accessed October 29, 2010).

³Yaakey, Randal, “Waterford Police Sued,” *The Oakland Press*, 2008, <http://deborahgordonlaw.com/media-2008.html#waterfordpolice> (accessed July 7, 2010); and No author, “Lafayette College Settle Sexual Harassment Case for \$1M,” *CampusSafetyMagazine.com*, April 26, 2010 (accessed October 29, 2010).

⁴Federal law prohibits discrimination based on race, color, religion, gender, national origin, age, disability, pregnancy, or genetic information (Civil Rights Act of 1964; Age Discrimination in Employment Act of 1967; Equal Pay Act of 1963; Americans With Disabilities Act of 1990; The Pregnancy Discrimination Act of 1978; The Family and Medical Leave Act of 1993; The Genetic Information Nondiscrimination Act of 2008). Most states have enacted similar legislation (for example, Wisconsin’s Fair Employment Law), and some states and municipalities have enacted legislation protecting additional classes, such as sexual orientation (for example, in the District of Columbia).

⁵Bonné, Jon, “Blogger Dismissed from Microsoft,” *Msnbc.com*, October 30, 2003, <http://www.msnbc.msn.com/id/3341689> (accessed May 11, 2010).

⁶Rose, Andrée; Howard Timm; Corrie Pogson; Jose Gonzalez; Edward Appel; and Nancy Kolb, *Developing a Cybervetting Strategy for National Security Positions* (Monterey, Calif., Defense Personnel Security Research Center: in press).

⁷A breakdown of the job sectors and occupations of participants can be found in Appendix B.

⁸The words “should” and “shall” are used throughout the guidelines. Reviewers suggested that we use either “should” or “shall,” but not both. This project’s approach is to provide guidelines that reflect either focus group consensus or a majority. Therefore, the authors have decided to leave the items unedited and use both words in the final document.

⁹Some focus group hosts were unable to attend the Capstone meeting. Their feedback was collected during a teleconference prior to the final meeting.

¹⁰The references to decisions of court cases presented in this document serve only as examples. These references should not be considered legal advice and the user is advised to consult with the appropriate legal office or policy officials to learn about the current status of law and its application to the specific facts at hand.

Unless otherwise noted, data for the court decisions provided in this document include official court documents, and case summaries provided by First Amendment Center, AELE Law Enforcement Legal Center, and Laura L. Scarry’s presentation “Free Speech in an Electronic World,” given at the Institute for Law Enforcement Administration, Plano, Texas, March 2010.

¹¹Zuckerberg, Mark, “The Facebook Blog: 500 Million Stories,” July 21, 2010, <http://blog.facebook.com/blog.php?post=409753352130> (accessed July 26, 2010).

¹²Rose, Andrée et al., *Developing a Cybervetting Strategy for National Security Positions*.

¹³Haefner, Rosemary, “More Employers Screening Candidates via Social Networking Sites,” *Careerbuilder*, June 10, 2009, <http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/?ArticleID=1337&cbRecursionCnt=1&cbsid=0b46ea4e1079427ea6ce9845d903d432-334081875-RP-4> (accessed January 5, 2010).

¹⁴Cross-Tab, *Online Reputation in a Connected World*, January 2010, <http://www.microsoft.com/privacy/dpd/research.aspx> (accessed July 7, 2010).

¹⁵This item was added to the guidelines during the last focus group.

¹⁶Federal Trade Commission, *Using Consumer Reports: What Employers Need to Know*, March 1999, <http://www.ftc.gov/bcp/edu/pubs/business/credit/bus08.shtm> (accessed August 9, 2010).

- ¹⁷Ehkle, Douglas, “The Fair Credit Reporting Act (FCRA) and the Investigation of Employee Misconduct.” February 1, 2004, <http://library.findlaw.com/2004/Feb/1/231211.html> (accessed April 11, 2010).
- ¹⁸Citizen Media Law Project Staff, “Hillstone Restaurant Group v. Pietrylo,” *Citizen Media Law Project*, July 13, 2009, <http://www.citmedialaw.org/threats/hillstone-restaurant-group-v-pietrylo> (accessed May 17, 2010).
- ¹⁹McCreary, Mark, “Privacy in Work-Related Matters Discussed in Social Networking Sites,” *Privacy Compliance and Data Security Blog*, April 27, 2009, <http://dataprivacy.foxrothschild.com/tags/pietrylo-v-hillstone-restaurant/> (accessed October 29, 2009).
- ²⁰Bouckaert, Jan and Degryse, Hans, *Opt in versus Opt Out: A Free-Entry Analysis of Privacy Policies* (Tilburg, Netherlands: Tilburg University, Center for Economic Research, December 16, 2005) <http://weis2006.econinfosec.org/docs/34.pdf> (accessed June 1, 2010); and European Union Data Protection Directive, 1995, <http://www.authernative.com/MandatoryRequirements.shtml#EUDPD> (accessed August 26, 2010).
- ²¹Gouras, Matt, “Montana City Asks Job Applicants for Facebook Passwords,” *The Huffington Post*, June 19, 2009, http://www.huffingtonpost.com/2009/06/19/montana-city-asks-job-app_n_218152.html (accessed October 20, 2009).
- ²²McCullagh, Declan, “Want a Job? Give Bozeman Your Facebook, Google Passwords,” *CNET News*, June 18, 2009, http://news.cnet.com/8301-13578_3-10268282-38.html (accessed June 14, 2010).
- ²³Thomas-Reseo, Chris, “Why My Google Search Results Are Different to Yours,” (September 24, 2008), <http://blogs.reseo.com/2008/09/why-my-google-search-results-are.html> (accessed June 14, 2010).
- ²⁴Eiserer, Tanya, “Dallas Police Officer’s Testimony May Taint Dozens of Cases,” *The Dallas Morning News*, April 30, 2009, www.law.pace.edu/files/archiveinthenews/dallasnews4-31.pdf (accessed August 24, 2010).
- ²⁵Phil Lynn, personal communication, June 10, 2010.
- ²⁶Dwyer, Jim, “The Officer Who Posted Too Much on MySpace,” *The New York Times*, March 10, 2009, http://www.nytimes.com/2009/03/11/nyregion/11about.html?_r=1 (accessed October 6, 2010); and Eric P. Daigle, “Chief’s Counsel: Social Networking Policies: Just Another Policy?” *The Police Chief* 77 (May 2010): 80–82, http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&issue_id=52010&category_ID=3 (Accessed August 23, 2010).
- ²⁷IACP Training Key 641, “Social Networking and Freedom of Speech” (June 2010); for information on how to obtain up-to-date training keys, please contact trainingkeys@theiacp.org.
- ²⁸Hooper, Laural L., Jennifer E. Marsh, and Brian Yeh, “Treatment of *Brady v. Maryland* Material in the United States District and State Courts Rules, Orders and Policies,” Report to the Advisory Committee on Criminal Rules of the Judicial Conference of the United States, October 2004, [http://www.fjc.gov/public/pdf.nsf/lookup/bradymat.pdf/\\$file/bradymat.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/bradymat.pdf/$file/bradymat.pdf) (Accessed June 14, 2010).
- ²⁹Scarry, Laura L., “Free Speech in an Electronic World,” presentation given at the Institute for Law Enforcement Administration, Plano, Texas, March 2010.
- ³⁰The Oyez Project, *San Diego v. Roe*, 543 U.S. 77 (2004), n.d. http://www.oyez.org/cases/2000-2009/2004/2004_03_1669 (accessed July 7, 2010).
- ³¹Paul, Richard A. and Lisa H. Chung, “Brave New Cyberworld: The Employer’s Legal Guide to the Interactive Internet,” *The Labor Lawyer* 24, no.1 (Winter 2008): 109–143.
- ³²Matteson, Cory, “Facebook Remarks Leave Nebraska Correction Officers Jobless,” *The Journal Star*, March 18, 2010, http://journalstar.com/news/local/crime-and-courts/article_3568155a-32ad-11df-9fb8-001cc4c002e0.html (accessed June 15, 2010).
- ³³Information labeled *sensitive* may vary from agency to agency. It is an agency’s responsibility to define this term.
- ³⁴International Association of Chiefs of Police, “Social Media Concepts and Issues Paper,” IACP National Law Enforcement Policy Center, September, 2010, <http://www.iacpsocialmedia.org/Portals/1/documents/social%20media%20paper.pdf> (accessed October 1, 2010).
- ³⁵Walsh, Susan, “EMT Fired after Posting Photos of Murder Victim on Facebook,” *San Francisco Examiner*, May 16, 2009, <http://www.examiner.com/x-10327-NY-Crime-Examiner~y2009m5d16-EMT-fired-after-posting-photos-of-murder-victim-on-Facebook> (accessed October 29, 2009).
- ³⁶Nyback, Glenn, “Former Staten Island EMT Arrested after Snapping Photos of Murder Victim,” *SILive*, June 4, 2009, http://www.silive.com/eastshore/index.ssf/2009/06/former_staten_island_emt_arres.html (accessed July 7, 2010).
- ³⁷Khalid, Kiran, “EMT Charged with Posting Photo of Corpse on Facebook,” *CNN*, June 4, 2009, <http://www.cnn.com/2009/CRIME/06/04/ny.facebook.corpse/index.html> (accessed October 29, 2009).
- ³⁸Rasin, Gregory I. and Ariane R. Buglione, “Social Networking and Blogging: Managing the Conversation,” *New York Law Journal*, July 27, 2009, http://www.law.com/jsp/nylj/PubArticleNY.jsp?id=1202432487473&Social_Networking_and_Blogging_Managing_the_Conversation&slreturn=1&hbxlogin=1 (accessed July 6, 2010).
- ³⁹Nix, Kelly, “Facebook Assailant Identified,” *The Carmel Pinecone*, 2009, <http://www.pineconearchive.com/091106/PCA.pdf> (accessed June 14, 2009); Nix, Kelly, “CHS Teacher Sues ‘John Doe’ over Fake Facebook Account,” *The Carmel Pinecone*, 2009, <http://www.pineconearchive.com/091016-3.htm> (accessed June 14, 2010).

⁴⁰Hennessey, Virginia, “Carmel High School Teacher Files Lawsuit against Online Impostor: Facebook Allegedly Used to Harass Carmel High Students,” *The Monterey County Herald*, October 15, 2009, http://www.montereyherald.com/ci_13566666?source=most_viewed (accessed October 16, 2009).

⁴¹Hennessey, Virginia, “Teacher Settles Cyberbully Lawsuit,” *The Monterey County Herald*, January 22, 2010, http://www.montereyherald.com/local/ci_14245525?nlick_check=1 (accessed January 22, 2010); Nix, Kelly, “Nonprofit Is Beneficiary of Facebook Lawsuit Settlement,” *The Carmel Pinecone*, January 29, 2010, <http://www.pineconearchive.com/100129PCA.pdf> (accessed June 14, 2010).

⁴²Facebook, “Help Center,” 2010, <http://www.facebook.com/help/?page=1020> (accessed June 15, 2010).

⁴³Garfinkel, Simson personal communication, July 27, 2010.

⁴⁴Moscaritolo, Angela, “Twitter Accounts Compromised in Torrent Site Scam,” *SC Magazine for Security Professionals*, February 4, 2010, <http://www.securecomputing.net.au/News/166357,twitter-accounts-compromised-in-torrent-site-scam.aspx> (accessed July 7, 2010); Perez, Sarah, “More Details on AT&T’s ‘Network Glitch’ That Caused Compromised Facebook Security,” *Read Write Web*, January 18, 2010, http://www.readwriteweb.com/archives/more_details_on_atts_network_glitch_which_compromised_facebook_security.php (accessed July 7, 2010); Acohidio, Byron, “How Cybercriminals Invade Social Networks, Companies,” *USA Today*, March 4, 2010, http://www.usatoday.com/money/industries/technology/2010-03-04-1Anetsecurity04_CV_N.htm (accessed July 7, 2010).

⁴⁵Hopkins, Curt, “Morpheme Tales: A (Reasonably) Comprehensive List of Fired Bloggers,” December 14, 2009, <http://morphemetales.wordpress.com/2010/07/18/a-fairly-updated-reasonably-comprehensive/> (accessed June 15, 2010).

⁴⁶David, Brennan, “Emotions Run High over Raid,” *The Columbia Times*, May 16, 2010, <http://www.columbiatribune.com/news/2010/may/16/emotions-run-high-over-raid/?news> (accessed August 9, 2010).

⁴⁷David, Brennan, “Officer Disciplined for SWAT-Related Comments: Officer Posted on Online News Story,” *The Columbia Times*, July 1, 2010, <http://www.columbiatribune.com/news/2010/jul/01/officer-disciplined-swat-related-comments/> (accessed August 9, 2010).

⁴⁸Federal Trade Commission, *Using Consumer Reports: What Employers Need to Know*, March 1999.

⁴⁹The people acknowledged in this section do not necessarily endorse these guidelines.

⁵⁰Chief Michael Force participated in the capstone focus group in place of Chief Ronald McBride. Dr. Dan Primorzc participated in the capstone focus group in place of Daniel Carlson.

Other Sources Consulted

Information and recommendations located in the following documents were used to draft the initial set of cybervetting guidelines and develop the glossary:

5 *C.F.R.* § 732.102, National Security Positions, Definition and Applicability.

“Online Networking, Texting and Blogging by Peace Officers: Part One – Impeachment, Policy & First Amendment Issues,” 2010 (4) AELE Mo. L. J. 201 ISSN 1935-0007.

32 *C.F.R.* § 154.3 Definitions.

“Adjudicative Desk Reference,” Version 3.1, September 2007, <http://www.rjhresearch.com/ADR/index.htm>. (accessed October 6, 2009).

Ahearn, Tom, “Background Checks and Social Networking Sites,” February 24, 2009, <http://www.pre-employ.com/blog/post/2009/02/Background-Checks-and-Social-Networking-Sites.aspx> (accessed August 28, 2009).

Air Force Public Affairs Agency Emerging Technology Division, “New Media and the Air Force,” <http://www.af.mil/news/newmedia/index.asp> (accessed March 3, 2010).

American Red Cross, *Social Media Handbook for Local Red Cross Units*, July 16, 2009, <http://sites.google.com/site/wharman/social-media-strategy-handbook> (accessed October 9, 2009).

Appel, Edward, *Mastering Internet Searching and Analysis for Investigations and Security*, September 15, 2008, <http://www.inamecheck.com/Mastering%20Internet%20Searching%20and%20Analysis%20for%20Investigations%20and%20Security%20Appel.pdf> (accessed October 20, 2009).

Appel, Edward, “Department of Defense Instruction on Internet Vetting (Draft).”

Bentley, Laura, “Screening Job Applicants with Social Networks? Establish Procedures First,” July 10, 2009, <http://www.itbusinessedge.com/cm/blogs/bentley/screening-job-applicants-with-social-networks-establish-procedures-first/?cs=34014> (accessed September 29, 2009).

Brandenburg, Carly, “The Newest Way to Screen Job Applicants: A Social Networker’s Nightmare,” *Federal Communications Law Journal* 60, no. 3 (2007): 597–626.

Brook Park Police Department, “Policy: Internet Sites/Web Pages/Social Networking,” 2009, www.iacpnet.org (accessed March 3, 2010).

Bureau of Justice Statistics, “All Terms and Definitions,” <http://bjs.ojp.usdoj.gov/index.cfm?ty=tda> (accessed December 31, 2009).

Cisco, “Cisco’s Internet Posting Policy,” March 24, 2008, http://blogs.cisco.com/news/comments/ciscos_Internet_postings_policy (accessed October 9, 2009).

- Chowdhry, Amit, "ESPN Limiting Employees to Social Networking Guidelines," August 7, 2009, <http://pulse2.com/2009/08/07/espn-limiting-employees-to-social-networking-guidelines/> (accessed October 6, 2009).
- Coutu, Diane et al., "We Googled You," *Harvard Business Review*, (June 2007): 37–47.
- Cumberland Police Department, "Professionalism," 2009 (retrieved through IACP Net, March 3, 2010).
- Dell, "Dell's Social Media Policies," <http://socialmedia.governance.com/policies.php> (accessed October 9, 2009).
- Defense Security Services, Personnel Security Clearances Office Information (PSCO), Department of Defense Directive 1334.1, "Wearing of the Uniform," August 11, 1969, <http://www.americanvolunteerreserve.org/directives/d13341p.pdf> (accessed December 22, 2009).
- E. J. DeLattre and Daniel L. Schofield, "Combating Bigotry in Law Enforcement," *FBI Law Enforcement Bulletin* 65, no. 6 (June 1996): 27–32.
- Department of Defense Instruction, "Public Release of User Identification for Information Systems (draft)," n.d.
- Dolan, Pamela L., "Update Employee Policies to Include Guidelines for Social Networking," *amednews.com.*, July 27, 2009, <http://www.ama-assn.org/amednews/2009/07/27/bica0727.htm> (accessed October 9, 2009).
- Doverspike, Dennis and L. Pamela Vaiana, "Googling for Job Relevant Information," *Assessment Council News*, October 2008, http://www.ipacweb.org/acn/acn_0810.pdf (accessed August 31, 2009).
- Emporia Police Department General Order Manual*, Social Networking #320, 2010 (retrieved through IACP Net, April 24, 2010).
- Executive Order 12968, Access to Classified Information, August 4, 1995, <http://www.fas.org/sgp/clinton/eo12968.html> (accessed October 18, 2010).
- Executive Order 10865, Safeguarding Classified Information within Industry, February 20, 1960, www.dod.gov/dodgc/doha/EO_10865-Amended.pdf (accessed October 18, 2010).
- Executive Order 10450, Security Requirements for Government Employees, April 27, 1953, <http://www.fas.org/irp/offdocs/eo/eo-13467.htm> (accessed October 18, 2010).
- Flynn, Dan, "Cyber-Vetting: A Growing Privacy Issue." Marietta, GA., Police Department, 2009.
- Garfinkel, Simson, *Database Nation* (Sebastopol, Calif.: O'Reilly & Associates, 2000.)
- Harpe, Lisa D., "Social Networks and Employment Law: Are You Putting Your Organization at Risk?" *People Click*, 2009, http://www.peopleclick.com/resources/wpaper/Social_Networks_Employment_Law_eBook.pdf (accessed October 15, 2009).
- Heathfield, Susan M., "Blogging and Social Media Sample Policy," *About.com.*, n.d. http://humanresources.about.com/od/policy/samples/a/blogging_policy.htm (accessed October 9, 2009).
- Hoang, Daniel, "Sample Social Networking Policy," March 6, 2009, <http://www.itbusinessedge.com/cm/docs/DOC-1257> (accessed October 8, 2009).
- "Truth or Dare: New Strategies for Screening Job Candidates," *HR.com.*, March 8, 2004, http://www.hr.com/SITEFORUM?&t=/Default/gateway&i=1116423256281&application=story&active=no&ParentID=1119278087386&StoryID=1119653413718&xref=http%3A//www.google.com/search%3Fhl%3Den%26rls%3Dcom.microsoft%25Aen-us%26rlz%3D117ADFA_en%26q%3DInternet+screening+job+applicants%26aq%3Df%26oq%3D%26aqi%3D (accessed September 29, 2009).
- Hyman, Jon, "Drafting a Social Networking Policy; 7 Considerations," June 10, 2009, <http://ohioemploymentlaw.blogspot.com/2009/06/drafting-social-networking-policy-7.html> (accessed October 8, 2009).
- "IBM Social Computing Guidelines," <http://www.ibm.com/blogs/zz/en/guidelines.html> (accessed October 6, 2009).
- Internal Revenue Service, "IRT – WBT Content 2009," 2009, www.irs.gov/files/filenode/social_network/training_course.pdf (accessed June 14, 2010).
- Lee, David and Shane Witnov, *Handbook on Conducting Research on Social-networking Websites in California*, December 1, 2008, http://www.law.berkeley.edu/files/Social_Networking_Website_Research-Handbook.pdf (accessed October 9, 2010).
- Leggitt, John S., Olga G. Schecter, and Eric L. Lang, *Cyberculture and Personnel Security Risk: Conceptual Framework and Trends*, Defense Personnel Security Research Center, Monterey, Calif., (forthcoming).
- Lenard, George, "Employers Using Facebook for Background Checking, Part I," December 5, 2006, <http://www.employmentblawg.com/2006/employers-using-facebook-for-background-checking-part-i/> (accessed June 27, 2010).
- Mann, Michael, "Google Your Applicants: Prospective Employees Are Increasingly Vetting Candidates' Web Pages," *New Jersey Law Journal* (June 2007).
- Minnesota National Guard Web Log Policy, http://www.minnesotanationalguard.org/press_room/blogs/MNNGBlogPolicy.pdf (accessed January 4, 2010).
- Mitchell, Julia E., "Warring Ideologies for Regulating Military Blogs: A Cyberlaw Approach for Balancing Free Speech and Security in Cyberspace," *Vanderbilt Journal of Entertainment and Technology Law* 9, no.1 (2006): 201–222.

Multi-National Corps – Iraq, Policy #9 - Unit and Soldier Owned and Maintained Websites, 2005, <http://thedonovan.com/archives/historystuff/Web%20log%20policy.pdf> (accessed October 6, 2009).

Obama-Biden Presidential Transition Team, Obama-Biden Job Questionnaire, 2008, http://usgovinfo.about.com/library/Obama_Administration_Questionnaire.pdf (accessed October 23, 2009).

Patel, Bijal J., “MySpace or Yours: The Abridgement of the Blogosphere at the Hands of at-will Employment,” *Houston Law Review* 44, no. 3 (2007): 778–812.

Pinkstone, Wayne E., “Social Networking Websites: Employment Law Pitfalls,” August 18, 2009, <http://media.straffordpub.com/products/social-networking-websites-employment-law-pitfalls-2009-08-18/speaker-handouts.pdf> (accessed October 9, 2009).

RightNow, “Social Web Employee Policy,” <http://www.rightnow.com/privacy-social.php> (accessed October 9, 2009).

Rosengarten, Michelle, “All Quiet on the Middle Eastern Front? Proposed Legislation to Regulate Milblogs and Effectuate the First Amendment in the Combat Zone,” *Cardozo Arts and Entertainment Law Journal* 24, no. 3 (2007): 1295–1358. <http://www.cardozoaelj.net/home/rosengarten.pdf> (accessed October 9, 2010).

Safe in YourSpace, “Yourspace Glossary of Terms,” <http://safeinyourspace.org/glossary.asp> (accessed October 19, 2009).

Schings, Stephanie, “SIOP Members Discuss Legal Implications of ‘E-Screening’ Job Applicants,” Society of Industrial and Organizational Psychology, May 27, 2009.

Schmidt, Wayne, “Online Networking, Texting and Blogging by Peace Officers: Part One – Impeachment, Policy & First Amendment Issues,” *AELE Monthly Law Journal* 201, no.4 (2010):201–209, <http://www.aele.org/law/2010all04/2010-04MLJ201.pdf> (accessed October 9, 2010).

Search Engine Watch, “Search Engine Watch SEM Glossary,” <http://searchenginewatch.com/define> (accessed October 19, 2009).

Shaw, Eric D., Lynn F. Fischer, and Andréé E. Rose, *Insider Risk Evaluation and Audit* (Monterey, Calif.: Defense Personnel Security Research Center, 2009.)

Shinder, Debra L., “10 Things You Should Cover in Your Social Networking Policy,” July 14, 2009, <http://blogs.techrepublic.com.com/10things/?p=875> (accessed October 9, 2009).

Social Media Marketing, “What Is Social Media?” <http://www.social-media-marketing.in> (accessed October 10, 2009).

Sprague, Robert, “Fired for Blogging: Are There Legal Protections for Employees Who Blog?” *University of Pennsylvania Journal of Labor and Employment* 9, no. 2 (2007): 355–387.

The Tech Terms Computer Dictionary, “Meta Search Engine,” TechTerms.com, <http://www.techterms.com/definition/metasearchengine> (accessed July 28, 2010).

University of California at Santa Barbara, “Social Networking on the Internet: Guide for UCSB Employees, Departments, and Registered Organizations,” <http://www.policy.ucsb.edu/policies/advisory-docs/social-networking-guide.pdf> (accessed October 6, 2009).

University of Texas, “Instructional Assessment Resources: Glossary,” n.d., <http://www.utexas.edu/academic/diia/assessment/iar/glossary.php> (accessed July 7, 2010).

Wisconsin National Guard, “OPSEC Concerns over Facebook and Twitter Use,” OPSEC Newsletter 09-01. 2009, <http://wisconsinmilitary.org/2009/09/17/family-and-military-opsec-concerns-over-facebook-and-twitter-use/> (accessed November 1, 2009).

Yahoo, “Yahoo Personal Blog Guidelines: 1.0,” <http://jeremy.zawodny.com/yahoo/yahoo-blog-guidelines.pdf> (accessed October 9, 2009).

Wikipedia, “Visual Search Engines,” http://en.wikipedia.org/wiki/Visual_search_engine (accessed July 1, 2010).

Urbandictionary.com, “Request a Friend,” <http://www.urbandictionary.com/define.php?term=request+a+friend> (accessed October 19, 2009).

APPENDIX A. SAMPLE FORMS

On-line and Internet History Supplemental Form

Please provide complete and accurate answers on this form to establish your qualifications. All answers will be subject to verification. When you have completed and reviewed your answers, save this form and submit it as you have been instructed.

Legal name (First, Middle, Last, Suffix)	
Nickname	
Alias (First, Middle, Last, Suffix)	
Gender	<input type="checkbox"/> Male <input type="checkbox"/> Female
Date of Birth	

Virtual Identities

Please provide e-mail addresses, screen names, nicknames, on-line names, handles and other identifiers you have used in the past seven years. Check if the address is shared with a spouse or another person.

E-mail address 1	<input type="checkbox"/>
E-mail address 2	<input type="checkbox"/>
E-mail address 3	<input type="checkbox"/>

More to enter? Use the additional information space at the end.

On-line activities

Please list any websites you have hosted, run, or participate in frequently, or other on-line activities that you have often done. List the name and URL, if known.

Name	URL
Website 1	http://
Website 2	http://
Website 3	http://

More to enter? Use the additional information space at the end.

If you have any information to add, please do so in the space below:

I certify that all of the information provided in this form is true and correct.

Submitted by:

First name	Middle name	Last name
------------	-------------	-----------

FIGURE A-1. SAMPLE PREEMPLOYMENT SCREENING QUESTIONNAIRE

Authorization for Disclosure of Social Networking Information

I, _____, give my permission for the Police Department Recruiting Division to have access to my personal social networking accounts. If my accounts are set to “private” I will log into the account in the presence of the Recruiting Officer and allow him or her to review the contents of the account(s). Access to the accounts(s) must be granted immediately upon request.

I understand that the information present on my person social networking account(s) is part of my background investigation. Any information that is racist, sexist or would bring discredit upon my candidacy for the position that I am applying for, may disqualify me from further consideration with the Police Department.

I understand that refusal to allow the Police Department Recruiting Division access to my personal social networking account(s) will disqualify me from further consideration for employment with the Police Department.

By signing this document, I am agreeing to provide the Police Department immediate access to my personal social networking accounts.

- I do not have a social networking account
- I authorize the Police Department access to my social networking accounts(s)
- I do not authorize the Police Department access to my social networking account(s)

_____ Candidate Signature	_____ Date
_____ Recruiting Officer Signature	_____ Date
Social Networking Account Name	_____
Additional Social Networking Account Names	_____

FIGURE A-1. (CONTINUED)

APPENDIX B. PROJECT PARTICIPANTS: JOB SECTOR AND OCCUPATION

Table B-1 presents the job sector of all project participants (excluding authors and other key staff). Of those who work within law enforcement (n = 170), 60 percent (n = 102) are sworn officers and chiefs of police (see Table B-2).

TABLE B-1. CYBERVETTING PROJECT PARTICIPANTS BY JOB SECTOR

<i>Sector</i>	<i>N</i>	<i>%</i>
Law enforcement	170	54.8
Other	68	22.0
Private	38	12.3
National Security	31	10.0
Unknown	3	1.0
Total	310	100.0

The total number of participants in Table B-1 differs from the total number of participants listed in the Acknowledgements Section because (1) a handful of participants participated in one or more project activities (for example, survey, focus groups, and consultations) and are listed more than once in the Acknowledgement Section, and (2) a handful of participants requested no attribution.

TABLE B-2. OCCUPATIONS WITHIN THE LAW ENFORCEMENT SECTOR

<i>Occupation</i>	<i>n</i>	<i>%</i>
Sworn officers	76	45.0
Chief of Police	26	15.3
IACP committee members*	13	7.7
Retired Chief	10	5.9
LE administrative staff	6	3.6
Federal LE	6	3.6
Human resources	5	3.0
Police academy personnel	3	1.8
LE personnel recruitment & selection	3	1.8
Corrections	2	1.2
Federal LE retired	2	1.2
Internet child exploitation	2	1.2
Internet investigations trainer**	2	1.2
IT/Forensic trainer	2	1.2
POST Board member	2	1.2
Public safety training	2	1.2
Analyst	1	0.6
Cadet	1	0.6
Computer Crime	1	0.6
Deputy Attorney General: Special Crimes Unit	1	0.6
Internet search specialist	1	0.6
LE contractor	1	0.6
LE psychologist	1	0.6
Prosecutor	1	0.6
Total	170	100.0

*Members may have more specialized law enforcement experience. A determination could not be made based on available information.

**Provides specialized training to law enforcement agencies

Table B-3 provides a breakdown of those professions classified as ‘Other.’

TABLE B-3. OCCUPATIONS WITHIN THE OTHER SECTORS

<i>Occupation</i>	<i>n</i>	<i>%</i>
Academic	21	30.9
<i>Information technology, privacy, media</i>	5	
<i>Information technology, media</i>	3	
<i>Management</i>	3	
<i>Psychology</i>	3	
<i>Criminal justice</i>	2	
<i>Information assurance</i>	1	
<i>Information technology, privacy</i>	1	
<i>IT</i>	1	
<i>Privacy</i>	1	
<i>Sociology</i>	1	
Attorney	11	16.2
<i>Employment</i>	6	
<i>Local government</i>	3	
<i>Intellectual property</i>	2	
Investigations: Preemployment screening	8	11.8
Human resources	5	7.4
Cyber security	4	5.9
Industrial organizational psychology consultant	3	4.4
Digital Forensics	2	2.9
IT	2	2.9
Personnel selection	2	2.9
Privacy	2	2.9
Anthropologist	1	1.5
Blogger	1	1.5
Emergency Management	1	1.5
Lexis Criminal Records	1	1.5
Social Media	1	1.5
Student	1	1.5
Superintendent	1	1.5
US Courts	1	1.5
Total	68	100.0

The sum may not equal 100% because of rounding.

APPENDIX C. CYBERVETTING GUIDELINES

Purpose and Scope

1. Law enforcement agencies should create a cybervetting policy that describes the purpose and scope of cybervetting. The policy should include information on the general types of information checked, collected, and used. This policy should be
 - a. applied uniformly to all applicants, candidates, and incumbents;
 - b. reviewed periodically by management and updated as needed;
 - c. reviewed and approved by the agency's legal counsel; and
 - d. made available to the public.
2. An agency's cybervetting policy should also apply to third parties who engage in work on behalf of that agency. Organizations that provide policing services (e.g., 9-1-1 dispatching and background investigations) should contractually agree to maintain consistency with the cyber-related policies an agency has in effect.

Notice and Consent

1. Law enforcement agencies shall inform applicants, candidates, and incumbents, in writing, that the Internet may be used to search for relevant information on them and that relevant online information may be collected and used to make employment decisions.
2. With the consent of applicants, candidates, and incumbents, law enforcement agencies may review online information about these individuals available on websites, where a subject's password is required to view content.
3. Applicants, candidates, and incumbents should be notified that failure to provide consent and/or deliberate concealment of or prevention of access to online content may have an impact on their employment status.

Lateral Police Transfers

1. Law enforcement agencies should notify lateral applicants that any information that is of a public safety concern or reflects upon their fitness for the position of a police officer may be shared with their current employer if the chief executive or designee at the agency conducting the vetting deems it necessary.

Cyber Searches

Personnel Authorized to Conduct Cybervetting

1. Personnel authorized to conduct cybervetting should be classified as holding a sensitive position and vetted in accordance with that classification.

2. Personnel authorized to conduct cybervetting should be notified that information collected from the Internet is confidential.

Employment Application or Background Questionnaire

1. The employment application or background questionnaire should ask job applicants, candidates, or incumbents:
 - a. For any e-mail addresses they have used over a period of time (period of time to be determined by the agency and the scope of its investigation). They should be notified that e-mail addresses will be used as search terms and that they are not required to disclose legally restricted e-mail addresses (for example, undercover or classified e-mail addresses).
 - b. For online screen names, handles, or nicknames used over a period of time (period of time to be determined by the agency and the scope of its investigation). They should be notified that screen names, handles, and nicknames will be used as search terms. Requests should be limited to user names and should not include information such as login credentials for online health care and banking.
 - c. For the websites or blogs where they are members, frequent, or contribute.
 - d. About any electronic content that would suggest a conflict of interest or could reflect negatively upon themselves or the potential employer. They should be afforded the opportunity to explain any potential concern.
 - e. If they have ever been a victim of identity theft, cyber bullying, or malicious postings. They should be afforded the opportunity to explain any potential concern they think might surface during the cybervetting process.
2. Law enforcement agencies should not ask for passwords.

Search Practices

1. Before drafting cybervetting practices, an agency should first ensure that policy makers know how social media tools work. Decision makers should stay abreast of policy and technical changes made by social networking sites.
2. Before drafting cybervetting practices, an agency should first ensure that policy makers know how cyber search tools work (for example, search engines and metasearches).
3. Applicants, candidates, and incumbents may be asked to access password-protected websites so that the recruiter or background investigator can review their profiles, blogs, or other online forums for disqualifying content.

4. Personnel conducting background investigations, including cybervetting, may contact any of the associates of applicants, candidates, or incumbents, including online friends.
5. E-mail addresses may be used as cyber search terms.
6. Screen names, handles, or nicknames may be used as cyber search terms.

Search Restrictions

1. Cybervetting may only be conducted on authorized workstations.
2. Cybervetting may not unlawfully bypass applicants', candidates', or incumbents' privacy settings on social networking sites.
3. Personnel conducting cyber searches shall use appropriate representations to obtain online information.

Search Results

1. Personnel authorized to conduct cybervetting shall document cybervetting methods and results.
2. Cybervetting results supplement background investigations and should be incorporated into the normal, lawful employment process.
3. Law enforcement agencies shall follow existing procedures that ensure information relating or pertaining to protected classes does not negatively impact hiring decisions.
4. Law enforcement agencies will report evidence of criminal activity uncovered during the cybervetting process to the appropriate law enforcement agency when doing so is consistent with existing policies or as required by law.

Training

Law enforcement agencies should ensure that appropriate training and mentoring is provided to all personnel involved in the cybervetting process (for example, policy makers, decision makers, and investigators). Training should address the following legal, ethical, and technical areas:

1. scope and purpose of cybervetting,
2. guidance on using Internet and social media tools,
3. capturing and retaining relevant information,
4. what constitutes prohibited grounds for discrimination, and
5. safeguarding data.

Social Media

Social Media Guidelines

1. Law enforcement agencies shall notify all personnel when a new cyber-related policy is implemented.
2. Absent exceptional circumstances, law enforcement personnel may not be prohibited from having a personal website or social networking profile.
 - a. Posting one's affiliation with a law enforcement agency; however, could have an effect on future work assignments (for example, undercover assignments).

3. Law enforcement personnel shall not post, transmit, or otherwise disseminate
 - a. any material that brings discredit to or may adversely affect the efficiency, reputation, or integrity of the agency.
 - b. photographs or depictions of themselves dressed in uniform and/or displaying official identification, patches or badges, trademarks, or logos without prior approval from the chief executive or designee.
 - c. sexual, violent, racial or ethnically derogatory comments, pictures, artwork, audio, video, or other material on the same website with any online material that references or may negatively affect the public perception of the agency.
 - d. text, pictures, audio, or videos of department training or work-related assignments without written permission from the chief executive or designee.
 - e. sensitive, confidential, proprietary, or classified information to which they have access due to their employment with the agency without prior permission from the chief executive or designee.
 - f. data from criminal or administrative investigations including photographs, videos, or audio recordings without prior permission from the chief executive or designee.
 - g. photographs of suspects, arrestees, or evidence, unless it is public information, without prior permission from the chief executive or designee.
 - h. personal statements about a use of force incident without prior permission from the chief executive or designee.
 - i. comments related to current or pending prosecutions without prior permission from the chief executive or designee.
 - j. images or details of restricted areas within the facility or its grounds without written permission from the chief executive or designee.
 - k. information about their agency's security procedures without written permission from the chief executive or designee.
 - l. information that could affect the safety or security of the agency or its employees.
 - m. details concerning locations and times of agency activities that are official and sensitive in nature without prior written authorization from the chief executive or designee.
 - n. images or any other materials, obtained during the course of their employment, that reflect the types of sensitive or proprietary technologies used by their agency without prior written authorization from the chief executive or designee.
 - o. comments on the operations of the agency, or specific conduct of supervisors or peers, that might negatively impact the public perception of the agency.
4. Personnel are expected to remain respectful of the agency and its employees, services, partners, and suppliers while blogging or posting in other online venues. Furthermore, employees may not reference agency partners or suppliers in an online forum without express consent of the chief executive or designee.

Monitoring

1. Law enforcement agencies should periodically inform personnel that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the agency at any time without prior notice.
2. Law enforcement agencies should periodically inform personnel that any information created, transmitted, downloaded, exchanged, or discussed on workplace equipment may be accessed by authorized personnel at any time without prior notice. Workplace equipment remains the property of the agency and no employee has a reasonable expectation of privacy with regard to that information. Agencies may want to document that personnel have received this notice.

Reporting

1. Law enforcement agencies may ask personnel to disclose any website(s) where they have posted information pertaining to their job or employment.
2. Law enforcement personnel who become aware of an Internet posting or website that is in violation of the department's policies shall immediately report that information to a supervisor.

Review of Data

1. When an agency becomes aware of personnel referencing the agency in a personal website, blog, or other online forum, authorized personnel may review the reference to ensure that it does not violate the agency's policy.
2. In response to concerns or complaints about online postings, the agency may accept, review, and evaluate third-party data (for example, coworker, concerned citizen, etc.).

Social Media Training for Personnel

1. Personnel should be notified that the department's standards of behavior, including harassment and anti-disparagement policies, apply to online behavior.
2. Law enforcement agencies should educate personnel on what constitutes an appropriate web presence as it relates to representing their agency and personal safety. Briefings should include but are not limited to
 - a. copyright, trademark, and other intellectual property laws and how they affect what employees can post online;
 - b. the impact Internet postings and other electronic communications have on people's ability to work in assigned positions (for example, undercover assignments), and active criminal cases (for example, impeached testimony);
 - c. personal and work-related information posted by employees, their families, or their friends may be misused; and
 - d. privacy settings at social media sites are constantly in flux. One should never assume that personal information posted at these sites is protected.

Authentication

Policy

1. Given (1) it is often difficult to know with certainty that information obtained from public areas on the Internet pertains to the actual person of interest, (2) people can maliciously place false information about people on the Internet, and (3) unintentional errors at certain public sites on the Internet are common, law enforcement agencies should attempt to verify information collected from the Internet is accurate and truly associated with the person of interest.

Practices

1. Law enforcement agencies should ask applicants, candidates, and incumbents to confirm the accuracy of any information found online. Applicants, candidates, and incumbents should be allowed to provide the names of references who can speak knowledgeably about the online information of concern.
2. Law enforcement agencies may provide a copy of online data used to make employment decisions to any individual who was the subject of the agency's cybervetting procedures and who makes a request for their information.
3. Law enforcement agencies should recommend candidates and incumbents correct erroneous information about them posted on the Internet.

Adjudication

Hiring, Retention, Promotion, and

Disciplinary Decisions

1. Hiring, retention, promotion, and disciplinary decisions may be affected by information found on the Internet.
2. Hiring, retention, promotion, and disciplinary decisions must be based on established criteria and processes.
3. Information, regardless of the source, should only be considered when it falls within the scope of the investigation, unless out-of-scope information reflects behaviors that could impact the ability of the applicant, candidate, or incumbent to perform his or her duties.

Incumbents

1. Law enforcement personnel
 - a. whose actions can be directly linked to websites that promote misconduct or bring discredit to the agency or a member of the agency, unless linked for official work-related purposes, should be investigated.
 - b. who violate their agency's social media policies shall be appropriately disciplined by the chief executive or designee.

Training

1. Law enforcement agencies shall ensure decision makers are properly trained on evaluating cyber search results.

Safeguarding Data

1. When collecting data, employers must consider the responsibilities associated with data collection, retention, and storage.
2. Cybervetting results should be safeguarded in a manner that is consistent with existing Human Resource policies and practices pertaining to employment and background investigation data.
3. The retention of cybervetting results should comply with existing document retention policies.
4. Law enforcement agencies should address the unauthorized disclosure of information obtained from the cybervetting process.
 - a. A process should be in place to inform applicants, candidates, and incumbents if their cybervetting results have been inappropriately disclosed.
5. Unauthorized disclosure should result in disciplinary action.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

**515 North Washington St.
Alexandria, VA 22314**

**1.800.THE IACP
www.theiacp.org**

©Copyright 2010