OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

CIVIL LIBERTIES AND PRIVACY GUIDANCE FOR INTELLIGENCE COMMUNITY PROFESSIONALS:

PROPERLY OBTAINING AND USING PUBLICLY AVAILABLE INFORMATION

July 2011

LEADING INTELLIGENCE INTEGRATION

FOREWORD

The Civil Liberties and Privacy Office of the Office of the Director of National Intelligence (ODNI) is pleased to present this *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicy Available Information*. This guidance was developed with great care, incorporating input from Intelligence Community (IC) legal counsel, officials responsible for civil liberties and privacy, and the open source community.

We trust this guidance will help IC professionals accomplish their missions. After all, protecting privacy and civil liberties as we carry out our intelligence duties is a mission imperative. We cannot do our jobs – we cannot use the tools and authorities granted to us – if we do not earn and retain the trust of the American people. We must demonstrate that we are worthy of that trust, and that we remain true to our oaths to support and defend the Constitution.

Alexander W. Joel
Civil Liberties Protection Officer

About Us: The Civil Liberties Protection Officer leads the ODNI's Civil Liberties and Privacy Office. This position was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The statutory duties of this official include ensuring that the protection of civil liberties and privacy is incorporated in the policies and procedures of IC elements. Accordingly, the mission of the Civil Liberties and Privacy Office is to lead the integration of civil liberties and privacy protections into the policies, procedures, programs, and activities of the ODNI and the IC.

INTRODUCTION

This Guidance, issued by the Office of the Director of National Intelligence, Civil Liberties and Privacy Office, is intended for personnel working in the United States Intelligence Community (IC) who obtain and/or use information that is available to the general public.

In today's rapidly changing world, IC professionals need guidance that facilitates a shared understanding of how the IC's rules and protections generally apply to their efforts to obtain and use information that is available to the general public, so that they can know when to seek legal and civil liberties/privacy advice, particularly when encountering new tools and sources of information.

IC professionals already receive training and guidance on the laws and policies that govern their activities. Why is specific guidance needed for obtaining and using information that is available to the general public?

First, with the rapid pace of change in technology and the availability of data, it is not always easy to determine what information is actually "publicly available" in online contexts. Moreover, IC elements have their own policies on how to protect privacy and civil liberties; it is helpful to have a shared understanding of how those protections generally translate into new environments.

New policies can also create challenges. For example, the IC's heightened emphasis on reaching out externally for expertise to inform analysis may encourage a broader spectrum of IC professionals than ever before to engage in a greater variety of external interactions.

Notwithstanding such changes, IC professionals remain bound to protect privacy and civil liberties of United States persons as they obtain and use information. As stated in the National Intelligence Strategy, intelligence officers should "exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people."

This document provides a framework for understanding how the IC's privacy and civil liberties protections apply to IC efforts to obtain and use information that is (or appears to be) publicly available. It also provides IC professionals with guideposts that will alert them when they need to consult with their OGCs and civil liberties and privacy officials.

Accordingly, this document is not a substitute for formal legal advice or policy guidance. It does not prescribe specific solutions for specific agencies. IC professionals must obtain such advice and guidance internally from their respective Offices of General Counsel (OGCs), compliance/oversight offices, and officials responsible for protecting privacy and civil liberties in their organizations.

THE IC'S CIVIL LIBERTIES PROTECTION INFRASTRUCTURE

Intelligence agencies protect privacy and civil liberties through an "infrastructure" of laws, policies, and oversight structures and processes. These include the Constitution and statutes of the United States – such as the Foreign Intelligence Surveillance Act (FISA), and the Privacy Act – and Executive Order 12333, "United States Intelligence Activities."

These are interpreted, applied, and overseen by a framework of agency OGCs, offices of inspector general, civil liberties and privacy officials, the Department of Justice, intelligence oversight offices, the Intelligence Oversight Board, and the legislative and judicial branches, as appropriate.

Executive Order 12333 sets forth what are commonly referred to as the IC's "U.S. person rules," embodied in implementing procedures approved by the head of the IC element and the Attorney General, in consultation with the DNI.

The Order requires members of the IC, when conducting intelligence activities, to "protect fully the legal rights of all United States persons [defined in the Glossary], including freedoms, civil liberties, and privacy rights guaranteed by Federal law."

The Order authorizes IC elements to collect, retain, and disseminate information about United States persons, in a manner consistent with each element's specific authorities, if it fits within certain categories, such as foreign intelligence and counterintelligence.

One such category is publicly available information.[1]

[1] Intelligence Community Directive (ICD) 301 establishes the National Open Source Enterprise and sets out the responsibilities for the oversight, management, and implementation of IC open source activities. ICD 301 defines open source information as "**publicly available information** that anyone can lawfully obtain by request, purchase, or observation."

FIVE FACTORS TO CONSIDER IN PROPERLY OBTAINING AND USING PUBLICLY AVAILABLE INFORMATION IN THE IC

To assist the IC professional, we have developed a shorthand, non-exhaustive list of factors to consider for properly obtaining and using publicly available information. These factors are discussed in greater detail in this document.

Factors to Consider in Properly Obtaining and Using Publicly Available Information:

1. Publicly Available – The information must be available to any member of the general public.

2. Lawfully Obtained – The information must be obtained lawfully under the Constitution and statutes of the United States, meaning, for purposes of this Guidance:

No special legal authorizations are needed, such as court orders or search warrants (if they're needed, then the information could still potentially be collected – it's just not "publicly available");

The *collection technique is authorized/appropriate* for IC professionals seeking publicly available information, rather than those IC professionals with specialized missions and authorities; and

The collection activity *does not focus on a person solely because of race, ethnicity, national origin, religion*, or protected First Amendment freedom of speech or assembly.

3. Affiliation – Prior to obtaining information, the professional has identified and complied with obligations, if any, to disclose affiliation with the IC.

4. **United States Person Information –** If the collection includes information concerning United States persons, then:

There must be a *valid mission* requirement for the information under Executive Order 12333; and

The information must be retained and disseminated in accordance with *Executive Order 12333, the Privacy Act*, and other applicable requirements.

5. Accuracy – Safeguards are in place to ensure that the information is used in a manner that satisfies IC standards for information accuracy, quality, and reliability.

Factor 1:

Publicly Available – The information must be available to any member of the general public.

Certain IC elements have promulgated procedures that define publicly available information for their agencies. For example, the *Attorney General's Guidelines for Domestic FBI Operations*, issued in September 2008, define "publicly available" as "information that has been published or broadcast for public consumption, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public."

Note that information that does not appear to be "publicly available" might still be available for collection to the IC through other lawful means.

Here are some guideposts for determining when information is "publicly available."

- Position or Status of Recipient. Is the information being made available to the IC professional solely because of the practitioner's *position or status* (i.e., as a government employee), or would it also be made available to any member of the public on request? Information obtained specifically because of one's position or status, as an IC professional would not be publicly available. Conversely, if such information is also provided to members of the public, it would be deemed publicly available.

Example: An IC analyst has developed an acquaintance with a university professor, and learns about a relevant, unpublished paper the professor has recently completed. The analyst notes that the professor is providing copies to attendees of a conference open to the public. She confirms with the professor that it is available to anyone who requests it, without restriction. This paper is *publicly available*, even though it is not yet a published document.

- Government Access. Is the information available to the IC professional by virtue of the practitioner's affiliation with a government agency? If being a government employee can open doors that are closed by law, policy or practice to members of the general public, the information sought is not "publicly available."

Example: A data company packages information products for different customers. It creates a package it believes will be particularly appealing to government agencies. In order to determine if the data is publicly available, IC professionals should review the data offerings contained in such products to determine whether they are "available to any member of the public" – and are being packaged together as a marketing mechanism – or whether they are only available to government agencies.

- Membership Organizations. Is the information distributed selectively, within a specific membership organization or club that is not open to the general public? While the government may well be able to obtain this information lawfully by specifically authorized means, if the information is not available to any member of the public upon request, payment of a fee or subscription, then it does not meet the definition of "publicly available."

- Purchase, Subscription, or Registration. Publicly available information includes information available by purchase or subscription. This also includes information that is provided free of cost, upon submission of contact information, such as an email address (make sure to review Factor 3, "Affiliation"). In all such cases, the key is whether the information is provided to any member of the public who provides the requested fee and/or subscription/registration information, without further selection/vetting by the provider.

- Online Information. Is the information posted online in a way that anyone can access, or is the content restricted in some way? An enormous amount of information is widely available on the Internet. A great deal of it is available to the general public, with no restrictions on access.

Some sites allow content providers to impose controls on access to content posted on the site. If those controls are intended to enable providers to implement purchase, subscription, and/or registration arrangements that facilitate distribution to the general public, the prior discussion should apply. On the other hand, care must be taken if the provider has implemented controls that limit access to certain individuals or groups only.

Example: An online network enables users to post content and establish connections with others. Users can adjust the network's settings to afford general access to the information they post, or they can adjust their settings to restrict who can see their postings. If the user has chosen to restrict access to her posted information so that the user grants access only to people the user already knows, or to members of a local club the user belongs to, then that information is not publicly available.

Factor 2:

Lawfully Obtained – The information must be obtained lawfully under the Constitution and statutes of the United States.

For purposes of properly obtaining publicly available information, this Guidance focuses on: (a) determining whether special legal authorizations are needed (e.g., court orders, warrants, etc.), (b) ensuring the collection technique is authorized/appropriate for someone seeking to obtain publicly available information (rather than for those IC professionals with specialized missions and authorities), and (c) ensuring that the activity does not focus on a person solely because of race, ethnicity, national origin, religion, or protected First Amendment speech or assembly.

Are special legal authorizations required?

Special authorizations may be needed to obtain certain information under the Constitution or applicable Federal statutes.[2] IC professionals should view the potential need for special authorizations as an indicator that the information sought is not "publicly available" and/or that the technique being used should be further reviewed by legal counsel/civil liberties and privacy officials.

- Fourth Amendment. Special authorization is required to obtain information protected by the Fourth Amendment. Courts have interpreted the Fourth Amendment's prohibition against "unreasonable searches and seizures" as applying to matters or venues in which individuals have a "reasonable expectation of privacy" – such as the content of a person's phone calls, personal correspondence, or personal computers, or what takes place in a person's home. Because such Fourth Amendment- protected information is subject to warrant or court order, it is not publicly available.

- Specific statutes. Similarly, Congress has enacted statutes that protect specific categories of data, and that prescribe specific mechanisms by which the government may obtain access to that data. For example, the Electronic Communications Privacy Act, the Telecommunications Act, and the Foreign Intelligence Surveillance Act, prohibit collection of certain electronic and stored communications except as a court specifically authorizes. Statutes also govern access to other categories of information, such as certain financial records, credit report information, medical records, educational records, DMV records, videotape rental records, and cable service subscriber records.[3] IC professionals should carefully review with legal counsel/civil liberties and privacy officials any efforts to obtain information in these categories.

[2] Executive Order 12333 will be mentioned below, and covered more fully under Factor 4.

[3] Records cited are protected by the following statutes: Right to Financial Privacy Act, Fair Credit Reporting Act, Health Insurance Portability and Accountability Act (the Privacy Rule), Family Educational Rights and Privacy Act, Driver's Privacy Protection Act, Video Privacy Protection Act, Cable Communication Policy Act.

Is the collection technique authorized/ appropriate for someone seeking to obtain publicly available information?

Here's another way of thinking about this issue: if the *technique or method* being considered seems to require specialized tradecraft or skills, or is typically used in clandestine ways, then that is an indicator that legal counsel should be consulted, or that the information being sought should be left to other officials experienced with seeking/obtaining appropriate authorization.

- Popular, Openly Used Techniques. Using techniques to obtain publicly available information that are commonly and openly used by members of the general public typically raise few issues. Such techniques include, for example, using popular online search engines in their intended ways, reading news media, attending conferences (subject to guidance in the "Affiliation" section), etc. This is in contrast to techniques used by "hackers" or others engaged in illicit activity to obtain information, even if such techniques may be openly discussed.

Example: Members of the public can use internet search engine features to search for news articles of interest. They can also "register" on public sites to access content by providing an email address so that the content provider can inform them of updates. By contrast, if a hacker posts instructions on a blog for how to penetrate a bank's online security, the bank's data does not become lawfully available as a result.

- Techniques that require tradecraft. Seeking to obtain information using a technique that involves the use of specialized intelligence tradecraft should signal the need for further internal review, which may involve consultation with legal counsel and/ or the need for special authorization. It may also involve referral of the matter to a different office/ organization with different authorities.

For example, observing individuals in a public place could evolve into "physical surveillance," depending on the circumstances.[4] Physical surveillance, like other potentially more intrusive techniques, if permitted, generally requires approvals under the agency's AG-approved United States person procedures.

[4] Executive Order 12333, Section 2.4, provides that implementing procedures "shall not authorize . . . [p]hysical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI" and "[p]hysical surveillance of a United States person abroad" except in certain specified circumstances.

- Contracting. Moreover, while members of the general public and/or private sector entities can enter into contracts with private investigators, data brokers, or others, to obtain information, IC professionals must remain mindful of Section 2.12 of E.O 12333, which provides: "No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order." Arrangements with third parties should be reviewed with counsel to verify compliance with applicable laws, even if such third parties market/package their services with labels such as "public records" or "publicly available information."

Does the activity comply with First Amendment and equal protection obligations?

Today's changing information environment involves large amounts of user-generated content posted on blogs, discussion forums, and the like. Such content may include details of users' religion, political interests, or affiliations. The public availability of this information does not affect the IC professional's obligation to honor Constitutional protections.

Constitutional issues can be complex, with no one-size-fits-all solutions. In seeking to obtain or use information believed to be publicly available, IC professionals should consult with legal counsel and civil liberties officials whenever they encounter such matters relating to United States persons or within United States jurisdiction.

- First Amendment. Americans have the right to speak their minds – in the town square or in the "blogosphere." By virtue of the First Amendment's guarantee of "free speech," they may make their views – however extreme – publicly available. The First Amendment also guarantees freedoms of association, religion, and assembly, which require limits/oversight on intelligence activities[5] The Attorney General's Guidelines for Domestic FBI Operations provide: "These Guidelines do not authorize investigating or collecting or maintaining information on United States persons *solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights* secured by the Constitution or laws of the United States."[6]

Example: A local citizens group has formed to protest the construction of a new government facility because of its potential impact on the local environment. It is using the Internet – including social networking tools – to publicize its positions, enlist support, and organize public protests. These protected First Amendment activities cannot be the sole impetus for collection. The

[5] The Constitution does not protect speech that incites people imminently to engage in violent acts; nor does provide an absolute right to associate with groups that actively advocate violence and acts of terrorism.

[6] Moreover, subsection (e)(7) of the Privacy Act prohibits federal agencies from maintaining any record describing how a U.S. citizen or resident alien exercises rights guaranteed by the First Amendment unless: expressly authorized by statute (e.g., IRS may maintain records on who advocates resistance to the tax laws); expressly authorized by the individual (e.g., individual requests religious accommodation); or within the scope of an authorized law enforcement activity (authorized criminal investigation/ or intelligence/ administrative activity).

fact that information about this group's activities is publicly available does not in itself mean that the government – or the IC – may collect that information or otherwise monitor the group's activities. A government entity may collect information about First Amendment activity only when valid and lawful reasons exist for collecting that information.

- Equal protection. Moreover, the Constitution guarantees equal protection to those within the jurisdiction of the United States. Care must be taken to avoid collecting publicly available information about a United States person (or group), based solely on race, ethnicity, or religion. In no event should ethnic, religious or racial stereotypes be relied upon for intelligence inquiry or analysis.[7]

Example: A group commits a terrorist act, and uses its own interpretation of a religious text as justification. Religious leaders condemn the act and its justification. Research on interpretations of the religious text may be conducted to better understand the new group's methods, ideology, and recruitment techniques. It would be impermissible stereotyping, however, to assume that an individual is affiliated in any way with the new terrorist group solely because he or she is a follower of the same religion.

[7] See Guidance Regarding the Use of Race by Federal Law Enforcement Agencies, 2003, United States Department of Justice Civil Rights Division. The Guidance makes clear as a general principle that reliance on stereotypes is prohibited by the Constitution. The Guidance uses the term "stereotype" to mean a "generalized assumption about persons" based on race or ethnicity.

Factor 3:

Affiliation - Prior to obtaining information, the professional has identified and complied with obligations, if any, to disclose IC affiliation.

Information that appears to be publicly available may be held by an organization, club, association, or other similar group, or may be available for discussion or distribution at a public meeting or event, either in person or online. This guidance has already highlighted the fact that information that is only available to *members of a closed organization* may not be "publicly available." What if, however, the organization itself appears to be open for public participation? What is the IC professional's obligation to disclose her affiliation?

Security concerns dictate that IC professionals should, generally speaking, take care about disclosing their affiliation with the IC. On the other hand, civil liberties considerations embodied in Executive Order 12333 dictate a degree of transparency. Section 2.9 of Executive Order 12333, Undisclosed Participation in Organizations within the United States, provides:

> No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures … approved by the Attorney General [in consultation with the DNI].

Individual agencies' AG-approved United States person procedures outline the circumstances in which an IC professional, including any contractor supporting an IC endeavor, may participate in undisclosed fashion. IC professionals should also consult related internal guidance to determine what additional approvals and restrictions might apply to the activity.

While the IC elements' individual AG- approved United States person procedures may differ, some general guideposts are offered.

- Location/type of organization. Executive Order 12333 applies to "any organization in the United States." Therefore, IC professionals should take care with participating in organizations located domestically. Note however, that an IC element's AG-approved United States person procedures and other guidance may apply the prohibition on undisclosed participation to organizations outside the United States as well.[8] Recall that under

[8] Procedure 10 of DoD's AG-approved United States person procedures, (DoD Directive 5240.1-R) prohibits undisclosed participation "by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community."

Executive Order 12333, a "United States person" may be an unincorporated association substantially composed of U.S. citizens or permanent resident aliens.

- Participation. Whether an IC professional's involvement or engagement with an organization constitutes "participation" under the Order depends on the circumstances. In general, IC professionals need not consider Executive Order 12333's "participation" guidelines when joining and participating in organizations solely for personal purposes.[9]

Note that activity undertaken within an organization on behalf of or for the benefit of an IC element after having joined the organization for one's own benefit may constitute "participation" for purposes of the procedures governing disclosure of affiliation.

Example: An IC element directs an employee to join an organization inside the United States to pursue an aspect of the IC element's intelligence mission. The employee is deemed to be "participating" and is subject to applicable disclosure of affiliation policies.

- Conferences, seminars and similar meetings. Attendance at conferences and other forums often involves formal registration, in the course of which organizational affiliation and personal biographical information may be requested. If attendance is permitted without disclosure of one's employment, participation is not considered "undisclosed." However, when registration is a condition of entrance, the IC member must consult with his/her element's counsel to determine how to proceed.

- Influencing the activities of the organization. Executive Order 12333 provides that participation under Section 2.9 is authorized only if essential for achieving lawful purposes, and may not be undertaken "for the purpose of influencing the activity of the organization or its members," with very limited exceptions.

- Online activities. Applying undisclosed participation rules to online activities is not always a straightforward process. Is the online website, network, or other forum an "organization in the United States" for purposes of the undisclosed participation rules? Does the proposed access/interaction constitute "participation?" Analogies to offline precedents may be helpful. Is the activity comparable to signing up for a magazine subscription? Or is it like joining a non-governmental organization, including attending meetings, interacting with members, and the like? IC professionals should consult closely with agency counsel, civil liberties and privacy officers, and internal guidance, to determine the appropriate steps to take.

[9] Procedure 10 of DoD 5240.1-R provides that the rule against undisclosed participation does not apply to "participation in organizations for solely personal purposes," clarifying that "[p]articipation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit."

Factor 4:

U.S. Person Information – If the collection includes information concerning United States persons, then it must be collected, retained, and disseminated consistent with Executive Order 12333 and the Privacy Act.

As discussed, Executive Order 12333 provides that IC elements may collect, retain, and disseminate information concerning United States persons only in accordance with procedures approved by the Attorney General, in consultation with the Director of National Intelligence, and in a manner consistent with each element's specific authorities. As further set forth in those procedures, the information must fall within one of the categories listed under Section 2.3 of Executive Order 12333 (e.g., foreign intelligence, counterintelligence, collected with consent, relevant to a lawful investigation, etc.). One of those categories is "information that is publicly available."

A threshold question is whether the information sought is "concerning a United States person." A *United States person* is defined by Executive Order 12333 as a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States except for a corporation directed and controlled by a foreign government or governments. This is a broad definition, and includes U.S. organizations and corporations, not just individuals.[10]

IC professionals should consider the totality of the information available to them in determining whether someone is a United States person. They should also consult their element's AG-approved United States person procedures, and legal counsel for further guidance regarding the presumptions and criteria for determining United States person status.[11]

When collecting information inside the United States or about United States persons abroad, IC professionals should use the "least intrusive collection techniques feasible."[12] Methods aimed at collecting publicly available information typically satisfy this requirement, since focusing on publicly available information is often less intrusive than other intelligence/investigative techniques. It is possible, however, that a chosen avenue for collecting publicly available information is unnecessarily intrusive, so IC professionals should take care to remember this requirement, and to consult with their organization's legal counsel for further guidance as needed.

[10] The Privacy Act, on the other hand, protects the information privacy of an individual, defined as "a citizen of the United States, or an alien lawfully admitted for permanent residence."

[11] For example, the current version of DoD Directive 5240.1-R provides that "[a] person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained."

[12] Executive Order 12333, Section 2.4.

There must be a valid mission requirement for the information

Nexus between conduct of an intelligence activity and agency mission is a fundamental premise of Executive Order 12333. Part 1 of the Order lays out the authorities and responsibilities of departments and agencies for conducting intelligence activities. Section 2.3 provides that IC elements are "only authorized to collect, retain, or disseminate information concerning United States persons … consistent with the authorities established in Part 1 of this Order."[13]

The requirement for nexus between intelligence activity and agency authority (or "mission"), applies to all the categories of information listed in Section 2.3 of Executive Order 12333. However, it is particularly important as applied to publicly available information. Without this "mission" requirement, Executive Order 12333 might be read to permit an IC professional to collect, retain, and disseminate – as part of agency intelligence activities – extensive official files assembled from publicly available information on everyone that the professional happens across – friends, neighbors, associates, celebrities, public figures.[14] Indeed, concerns have been expressed that intelligence agencies could build extensive dossiers on Americans without special authorization, simply by using publicly available information.

IC professionals may not engage in such conduct. They must tie their activities – including obtaining and using publicly available information – to an authorized mission specific to their element, as set forth in Part 1 of Executive Order 12333.[15]

Example: Much information about individuals circulates on the Internet – some may be public figures, others may be private individuals who have posted information about themselves or others. Although this information is available to the general public, an IC element can only collect and retain that information if it relates to an IC element's mission under Part 1 of Executive Order 12333. By contrast, publicly available information is frequently available about individuals who are being investigated/arrested for national/homeland security-related offenses. Such information is likely to be closely related to the missions of various IC organizations.

The degree of relationship to agency mission will depend on the circumstances and on the agency's procedures.

United States person information must be retained and disseminated in accordance with Executive Order 12333.

Having determined that information may properly be obtained, the practitioner should understand applicable federal record-keeping and dissemination requirements. IC professionals must ensure that information is being retained and disseminated properly.

[10] Section 1.7 of Executive Order 12333 focuses specifically on the authorities of IC elements.
[14] The Privacy Act, discussed later, provides safeguards as well.
[15] Moreover, IC professionals should be aware that their agencies may have imposed other limitations on collecting publicly available information under Executive Order 12333 (e.g., restrictions on collection activity concerning the "domestic activities of United States persons"; requirements for a "foreign connection," and the like).

- Retaining information under Executive Order 12333 involves consideration of the same types of issues already discussed. Is this information "concerning a United States person?" If so, is it "publicly available"? Does it relate to the IC element's mission? IC elements have developed different procedures for determining the period of time that an IC element has for making these determinations, recognizing that immediate determinations cannot feasibly be made in all cases. Internal agency guidance must be consulted in order to determine what process should be followed to review and retain United States person information under applicable AG-approved United States person procedures. Once it is determined that information can be retained, records retention policies should be followed (more on this later).

- Disseminating information under Executive Order 12333. Once information concerning United States persons has been properly retained, it may be disseminated pursuant to the element's AG-approved United States person procedures. As a general matter, if the US person information meets the retention criteria because it is related to the IC element's mission and fits one of the permissible retention categories under EO 12333, it may be disseminated. In addition, some procedures or situations require IC professionals to make some kind of determination about the dissemination (generally involving the recipient organization) – even of publicly available information.[16] Some general points (should be checked with internal guidance, which may vary by agency):

  - De-Identification. Disseminations can generally be facilitated by "de-identifying" (or anonymizing) the specific information "concerning a United States person" (e.g., replacing it with generic, non-identifying terminology).

  - Within the IC. Generally allowed to enable the IC element to determine whether it can retain the information pursuant to its procedures- but consult internal guidance first.

  - Other Federal Agencies. Generally allowed to agencies that have a need for the information in performance of a lawful governmental function, subject to agency-specific procedures/criteria.

  - Other Entities. Authorities/procedures differ by IC element (particularly with respect to the Privacy Act – see next section).

  - Violations of Law/Protection of Life/Safety. Generally permitted, pursuant to specific procedures/authorizations.

[16] Note also that "dissemination" of information under Executive Order 12333 may, under certain circumstances, constitute a "disclosure" of records under the Privacy Act, for which there should have been published an appropriate routine use – more on this below.
[17] Certain departments and agencies may extend (by policy), specific Privacy Act treatment to personal information of non-United States persons, and pursuant to such policy, commingle the records of non-citizens with those of citizens and resident aliens (i.e., in a "mixed system"). An IC professional should understand whether her agency subscribes to such a policy.

Maintaining and disclosing records under the Privacy Act.

The Privacy Act provides U.S. citizens and permanent resident aliens ("individuals")[17] certain rights and assurances, and imposes on the government certain obligations, when federal executive branch agencies collect, maintain, and use their personal information.

- Maintaining records under the Privacy Act. Any records about U.S. citizens or resident aliens (even if collected from publicly available sources) that the federal government maintains and retrieves by name or a unique personal identifier are part of a "system of records" under the Privacy Act. The key for IC professionals is determining whether information they are retaining is part of such a "system of records." If so, they must handle those records in accordance with specific administrative requirements of that Act, or risk civil and criminal penalties.[18] Privacy Act records should be retained in accordance with applicable retention policies (more on this below).

- Disseminating Privacy Act records. Additionally, all agencies, regardless of the nature of the information they maintain, should protect records held in a Privacy Act system of records from improper disclosure. The Privacy Act prohibits federal agencies from disclosing an individual's records from a Privacy Act system of records except with the consent of the individual to whom the record pertains or as permitted by one of twelve specific circumstances, including a published "routine use."[19]

An IC user of publicly available information that is held in a Privacy Act system of records should ensure that disclosures to any recipient outside the agency are consistent with the agency's implementation of the Privacy Act (e.g., "routine use" statements).[20] Agency-internal disclosures should be limited to those individuals who have a need for the records or a need to examine the records in performing their official duties.

Additional Considerations for Retaining and Disseminating Information.

- Records retention periods. The IC professional should consult with records management personnel (e.g., information management officers) to apply appropriate records retention and disposition policies.[21] Once the period of authorized retention expires, information should be removed according to applicable procedures and records control schedules.

[18] In general, IC professionals working with Privacy Act systems of records should handle any publicly available information that becomes part of those records in accordance with the training and guidance provided to them for those systems of records. Specific questions should be directed to privacy officials, records management personnel, and legal counsel.

[19] A "routine use" under the Privacy Act is a statement published in the Federal Register describing circumstances in which the agency may disclose a record to a user outside the agency. 5 U.S.C. 552a(e)(4).

[20] For IC elements, routine use statements will likely already cover common sharing avenues/partners, such as sharing within the IC and with intelligence customers.

[21] The Federal Records Act, 44 U.S.C. 3301 et seq., requires agencies to create and maintain accurate and complete records of the agency's functions and activities, and to properly dispose of documentary materials that are no longer needed to conduct business.

- Potential for broad distribution. Because publicly available information is likely to be included in unclassified intelligence products, IC professionals should be mindful that such products may be distributed to non-traditional IC customers, who may lack the background that experienced IC customers have in understanding/contextualizing IC reporting. The fact that an IC element has created a product focusing on a United States person – even if it relies on publicly available information – could itself be viewed as significant, with potential reputational or other consequences for that person.

- Other privacy requirements. IC professionals should remain mindful of other privacy-related requirements for retaining and disseminating information. For example, if the IC professional is working with a system for which a "privacy impact assessment" (PIA) has been performed pursuant to the E-Government Act of 2002 (for systems containing "personally identifiable information"), then that PIA might identify additional policies or measures to be followed. In addition, agreements and other instruments may accord additional protections to certain datasets, particularly in the context of sharing information between agencies.[22]

[22] For example, the "ISE Privacy Guidelines" (available at www.ise.gov) provide that information about non-United States persons can be covered by its information sharing privacy safeguards if so directed by executive order, international agreement, or similar instrument.

Factor 5:

Accuracy – Safeguards are in place to ensure that the information is used in a manner that satisfies IC standards for information accuracy, quality, and reliability.

Applying the IC Analytic Standards, which are the "core principles of the analytic craft,"[23] helps maintain alignment with civil liberties and privacy principles. Both emphasize the importance of objectivity, avoiding bias, and focusing on the quality and reliability of underlying information. This is particularly important when obtaining and using publicly available information, the accuracy and reliability of which has sometimes been questioned.

The IC Analytic Standards emphasize, among other things, that analysts: should perform their functions from an unbiased perspective, free of emotional content; provide objective assessments informed by available information that are not distorted or altered with the intent of supporting a particular policy or political viewpoint; be informed by all relevant information that is available to the analytic element; properly describe the quality and reliability of underlying sources; note sources of uncertainty, including information gaps and contrary reporting.

These standards are consistent with privacy and civil liberties principles, such as the mandate of Executive Order 12333 to use all means to obtain "reliable intelligence information," and with the Privacy Act's requirement to make reasonable efforts to assure records are accurate prior to disclosure/dissemination.

Considerations:

- As alluded to above, it is important to apply the IC Analytic Standards to the use of publicly available information.
- In the broad "public marketplace of ideas," IC professionals should keep in mind that publicly available information may reflect bias, and/or may be distorted by an intent to support a particular policy or political viewpoint. In particular, be aware that terms/labels used in public discourse by particular authors/groups might not be appropriate to replicate in the same context within the IC, since they might label/stigmatize larger communities in unintended ways.
- Before using information obtained from commercial data sources (e.g., data brokers/resellers or other "pay to play" services), understand that they may obtain information from secondary/indirect sources, and may have varying approaches to data quality. Be wary of conclusory representations from such services about the "publicly available" nature of the data they provide.

[23] Intelligence Community Directive 203, Analytic Standards. The standards are objectivity, independent of political considerations, timeliness, based on all available sources of intelligence, and exhibits proper standards of analytic tradecraft (with eight sub-components).

GLOSSARY

- *"Individual"* - for purposes of the Privacy Act, is a United States citizen or a lawful permanent resident.

- *"Publicly available information"* – no common definition across the IC. Defined in the AG Guidelines for the FBI as information that has been published or broadcast for public consumption, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

- *United States person* - defined by Executive Order 12333 as:

  - a United States citizen,
  - an alien known by the intelligence element concerned to be a permanent resident alien,
  - an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or
  - a corporation incorporated in the United States except for a corporation directed and controlled by a foreign government or governments.

NOTES

NOTES

NOTES

Office of the Director of National Intelligence
Washington, D.C.