

**EXHIBIT N**

**GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION  
BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES  
OF INFORMATION IN DATASETS CONTAINING  
NON-TERRORISM INFORMATION**

**I. Background**

A. Pursuant to section 119(d) of the National Security Act of 1947, as amended, the National Counterterrorism Center (NCTC) shall “serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism.” NCTC shall also “serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support”; ensure that agencies “have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis”; and “ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities.” Furthermore, any agency “authorized to conduct counterterrorism activities may request information” from NCTC “to assist it in its responsibilities.” *Id.* § 119(e)(2). Finally, the Director of National Intelligence (DNI) also has significant responsibilities for information sharing. He has “principal authority to ensure maximum availability of and access to intelligence information” within the Intelligence Community (IC). *Id.* § 102A(g)(1). When he establishes standards for facilitating access to and dissemination of information and intelligence, the DNI should give “the highest priority to detecting, preventing, preempting and disrupting terrorist threats and activities.” Executive Order 12333 § 1.3(b)(6)(A).

B. NCTC’s analytic and integration efforts concerning terrorism and counterterrorism, as well as its role as the central and shared knowledge bank for known and suspected terrorists, at times require it to access and review datasets that are identified as including non-terrorism information in order to identify and obtain “terrorism information,” as defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended.<sup>1</sup> “Non-

---

<sup>1</sup> “The term ‘terrorism information’—

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(iii) communications of or by such groups or individuals; or

(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information.” 6 U.S.C. § 485(a)(5).

## UNCLASSIFIED

terrorism information” for purposes of these Guidelines includes information pertaining exclusively to domestic terrorism, as well as information maintained by other executive departments and agencies that has not been identified as “terrorism information” as defined by IRTPA. Included within those datasets identified as including non-terrorism information may be information concerning “United States persons,” as defined in Executive Order 12333 of December 4, 1981, as amended. The President authorized the sharing of terrorism information in Executive Order 13388 of October 25, 2005, and required that agencies place the “highest priority” on the “interchange of terrorism information” in order to “strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America.” That order further requires that the “head of each agency that possesses or acquires terrorism information . . . shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency,” consistent with law and statutory responsibilities. In the National Security Act of 1947, as amended, Congress recognized that NCTC must have access to a broader range of information than it has primary authority to analyze and integrate if it is to achieve its missions. The Act thus provides that NCTC “may, consistent with applicable law, the direction of the President, and the guidelines referred to in section 102A(b), receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.” National Security Act of 1947, as amended, § 119(e). Further, the Act envisions that NCTC, as part of the Office of the Director of National Intelligence (ODNI), *id.* § 119(a), would have the broadest possible access to national intelligence relevant to terrorism and counterterrorism. Section 102A(b) of the National Security Act of 1947, as amended, provides that “[u]nless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.”

C. These Guidelines are established between the Attorney General and the Director of National Intelligence pursuant to section 102A(b) of the National Security Act of 1947, as amended, to govern the access, retention, use, and dissemination by NCTC of terrorism information that is contained within datasets maintained within other executive departments or agencies that are identified as including non-terrorism information. These Guidelines do not supersede the arrangements in place under the Memorandum of Agreement for the Interagency Threat Assessment and Coordination Group (ITACG). *See* Homeland Security Act of 2002, as amended, section 210D, and the September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group (hereinafter the “ITACG MOA”). The procedures for the ITACG MOA will be implemented consistent with these Guidelines. These Guidelines also constitute procedures pursuant to section 2.3 of Executive Order 12333 for NCTC’s access to and acquisition of data concerning United States persons within the datasets explicitly covered by these Guidelines, and the retention and dissemination of such information from these datasets. The Attorney General-approved procedures pursuant to section 2.3 generally governing NCTC’s and ODNI’s access and acquisition activities (reference (o), below) are hereby superseded insofar as they apply to

## UNCLASSIFIED

NCTC's retention, use, and dissemination of data and datasets governed by these Guidelines. NCTC's retention, use, and dissemination of information contained in the datasets governed by these Guidelines and all other NCTC activities remain subject to all other applicable laws and regulations. The terms and conditions of each specific information access or acquisition (hereinafter "Terms and Conditions") from another department or agency (hereinafter a "data provider") shall be developed in accordance with the provisions in section III.B.2 below, and shall be consistent with the Information Sharing Environment (ISE) guidelines issued pursuant to section 1016 of the IRTPA, to include the guidelines to protect privacy and civil liberties in the development and use of the information sharing environment.

## II. References

- a) National Security Act of 1947, as amended
- b) Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended
- c) Homeland Security Act of 2002, as amended
- d) Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)
- e) 18 U.S.C. § 2332b(f) (Acts of terrorism transcending national boundaries—investigative authority)
- f) Executive Order 12333 of December 4, 1981, as amended, "United States Intelligence Activities"
- g) Executive Order 13388 of October 25, 2005, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"
- h) Intelligence Community Directive (ICD) 501 of January 21, 2009, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community"
- i) ICD 503 of September 15, 2008, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation"
- j) Director of Central Intelligence Directive (DCID) 6/3 of June 5, 1999, "Protecting Sensitive Compartmented Information within Information Systems," appendix E (or successor ICD and Policies)
- k) DCID 6/6 of July 11, 2001, "Security Controls on the Dissemination of Intelligence Information," (or successor ICD and Policies)
- l) December 4, 2006 Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment
- m) March 4, 2003 Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing
- n) September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group
- o) The Attorney General-approved procedures promulgated through Central Intelligence Agency Headquarters Regulation 7-1 of December 23, 1987, "Law and Policy Governing the Conduct of Intelligence Activities," as adopted by ODNI/NCTC, including any successor procedures (hereinafter "NCTC's EO 12333, § 2.3 Procedures")
- p) National Counterterrorism Center Information Sharing Policy of February 27, 2006, "Rules of the Road" (NCTC Policy Document 11.2) (or successor Policy)

## UNCLASSIFIED

- q) National Counterterrorism Center Role-Based Access Policy of July 13, 2009 (NCTC Policy Document 11.7) (or successor Policy)
- r) ODNI Instruction 80.05, Implementation of Privacy Guidelines for Sharing Protected Information, September 2, 2009 (hereinafter "ODNI ISE Privacy Instruction")
- s) ODNI Instruction 80.02, Managing Breaches of Personally Identifiable Information, February 20, 2008.

### III. Guidelines

#### A. Authority for and Scope of NCTC Data Access and Acquisitions

1. *Purpose and Authority.* NCTC's access to, and acquisition, retention, use, and dissemination of, information covered by these Guidelines will be for authorized NCTC purposes. Pursuant to Executive Order 13388 and consistent with the National Security Act of 1947, as amended, and the March 4, 2003 Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, NCTC shall be afforded prompt access to all federal information and datasets that may constitute or contain terrorism information. NCTC may access or acquire datasets that may constitute or contain terrorism information, including those identified as containing non-terrorism information, such as information pertaining exclusively to domestic terrorism and other information maintained by executive departments and agencies that has not been identified as terrorism information, in order to acquire, retain, and disseminate terrorism information pursuant to NCTC's statutory authorities consistent with these Guidelines.

2. *United States Person Information.* These Guidelines permit NCTC to access and acquire United States person information for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,<sup>2</sup> used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures below. Information is "reasonably believed to constitute terrorism information" if, based on the knowledge and experience of counterterrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information.

3. *Erroneously Provided Information and Errors in Information.* Any United States person information that has been erroneously provided to NCTC will not be retained, used, or disseminated by NCTC. Such information will be promptly removed from NCTC's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General. Information in NCTC systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and the data provider shall be notified of the error when feasible.

---

<sup>2</sup> For purposes of these Guidelines, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with NCTC's records retention policies.

## UNCLASSIFIED

### 4. *Applicable Laws and Policies.*

a) NCTC will access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. These Guidelines do not apply to information the retention, use, and dissemination of which is governed by court order or court-approved procedures.

b) NCTC shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. NCTC users of acquired information will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, to applicable ODNI Instructions, and to additional audit and oversight authorities and requirements, as applicable. In implementing these Guidelines, NCTC shall consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, as appropriate.

5. *Responsibility for Compliance.* The Director of NCTC, in consultation with the ODNI Office of General Counsel, shall be the responsible official for ensuring that NCTC complies with these Guidelines. The ODNI Civil Liberties Protection Officer shall oversee compliance with these Guidelines and compliance with other applicable laws, regulations, guidelines, and instructions as they relate to civil liberties and privacy.

### **B. General Procedures for NCTC Data Access and Acquisitions**

1. *Identification of Datasets.* NCTC will coordinate with the data provider to identify datasets that are reasonably believed to contain terrorism information, including those identified as containing non-terrorism information.

2. *Establishing Terms and Conditions for Information Access.*

a) For access to or acquisition of specific datasets, the DNI, or the DNI's designee, shall collaborate with the data provider to identify any legal constraints, operational considerations, privacy or civil rights or civil liberties concerns and protections, or other issues, and to develop appropriate Terms and Conditions that will govern NCTC's access to or acquisition of datasets under these Guidelines. If either party believes that the Terms and Conditions do not adequately address the matters identified during that collaboration, that party may raise those concerns in accordance with the procedures in section III.B.2(d), below. These Guidelines do not alter any other obligations of a data provider to provide information to the DNI or NCTC. All Terms and Conditions shall incorporate these Attorney General-approved Guidelines, and shall ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that (i) protects privacy and civil liberties and information integrity and security, and (ii) is in accordance with applicable laws, regulations, guidelines and instructions (including the ODNI ISE Privacy Instruction). NCTC and the data provider will establish procedures to ensure the

## UNCLASSIFIED

data provider notifies NCTC of any information the data provider believes, or subsequently determines to be, materially inaccurate or unreliable. NCTC will ensure mechanisms are in place at NCTC to correct or document the inaccuracy or unreliability of such information, and supplement incomplete information to the extent additional information becomes available. NCTC will work with the data provider to ensure that data acquired by NCTC under these Guidelines is updated and verified throughout its retention and use by NCTC, in accordance with the data quality, data notice, redress, and other applicable provisions of the ODNI ISE Privacy Instruction.

b) NCTC shall consult with the data provider to identify and put in place additional measures as necessary to honor obligations under applicable international agreements governing the information.

c) Any safeguards, procedures, or oversight mechanisms that go beyond those specified in these Guidelines shall be documented in the Terms and Conditions, and may include protections for sensitive sources and methods, pending investigations, law enforcement equities, foreign government interests, privacy and civil liberties, and similar considerations that apply to the use of the information. Any additional protective measures – such as the degree of advance coordination, if any, for dissemination of information obtained from a data provider – shall also be specified in the Terms and Conditions.

d) If the head of the department or agency providing the information or the DNI objects to providing data to NCTC, objects to the “track” under which NCTC intends to acquire the data, or objects to the Terms and Conditions developed after consultation (e.g., he or she believes that the Terms and Conditions do not adequately ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that protects privacy and civil liberties and information integrity and security; do not adequately address operational equities; unnecessarily restrict sharing and use of the information; or are not in accordance with applicable laws, international agreements, and regulations), the head of the department or agency or the DNI may raise any concerns, in writing, with the other party. The head of the department or agency and the DNI shall attempt to resolve any such concern. Failing resolution, either party may refer a dispute concerning constitutional or other legal matters to the Attorney General and may seek the resolution of any other disputes through the National Security Council process. In connection with such disputes, the Attorney General or National Security Council may seek the advice of the Privacy and Civil Liberties Oversight Board.

3. *Training.* NCTC shall ensure that all NCTC employees, NCTC contractors, and detailees and assignees to NCTC from other agencies (hereinafter “NCTC personnel”) provided access to datasets under these Guidelines receive training in the use of each dataset to which they will have access to ensure that these personnel use the datasets only for authorized NCTC purposes and understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each such dataset. These personnel will also receive ongoing training to ensure understanding of these Guidelines and civil liberties and privacy expectations and requirements involved in the access to and use of datasets governed by

## UNCLASSIFIED

these Guidelines. The training required by this paragraph shall be in person whenever practicable and refreshed at least annually.

4. *Authorized Uses of Information.* Subject to any additional protections, requirements, or provisions in applicable Terms and Conditions, terrorism information, including terrorism information concerning United States persons, properly acquired and retained by NCTC may be used for all authorized NCTC purposes. These include, but are not limited to: analysis and integration purposes, inclusion in finished analytic products and pieces, enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support, strategic operational planning, and appropriate dissemination to Intelligence Community elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth in sections III.C and IV below, and any additional protections or provisions shall be specified in the Terms and Conditions.

5. *Information Access Requests.* For information acquired pursuant to the tracks outlined in section III.C below, it shall be the responsibility of the data provider to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement is agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and specified in the Terms and Conditions for that information.

### C. Specific Procedures for NCTC Data Access and Acquisitions

*General.* NCTC may acquire information contained within datasets governed by these Guidelines in one or more of the three ways outlined below. NCTC, in coordination with the data providers, will determine which information acquisition track, or tracks, provides the most effective means of ensuring NCTC access to terrorism information contained in the relevant datasets, consistent with the protection of privacy and civil liberties of United States persons, and any applicable legal requirements affecting provision of the specific data.

#### 1. Track 1 Information Acquisition: Account-Based Access

a) *Type of Access.* NCTC personnel may be provided account-based access to the datasets of data providers that contain or may contain terrorism information (hereinafter "Track 1" access).

b) *Standard.* NCTC will access information in such datasets identified as containing non-terrorism information only to determine if the dataset contains terrorism information. NCTC may acquire, retain, use, and disseminate terrorism information for all authorized NCTC purposes, as described in these Guidelines. If the information acquired by NCTC is subsequently determined not to constitute terrorism information, NCTC will promptly purge any information the retention, use, or dissemination of which is not authorized by sections IV and V below.



## UNCLASSIFIED

c) *Terrorism Datapoints.* Consistent with section 119 of the National Security Act of 1947, as amended, and section 1016(a)(5) of the IRTPA, as amended, the initial query term for NCTC Track 1 access shall be a known or suspected terrorist identifier or other piece of terrorism information (hereinafter “terrorism datapoints”). In order to follow up on positive query results, subsequent terrorism datapoints may be used to explore a known or suspected terrorist’s network of contacts and support. NCTC’s activities in Track 1 shall be designed to identify information that is reasonably believed to constitute terrorism information. NCTC is not otherwise permitted under these Guidelines to query, use, or exploit such datasets. For example, analysts may not browse through records in the dataset that do not match a query with terrorism datapoints, or conduct pattern-based queries or analyses without terrorism datapoints.

d) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that terrorism datapoints and matching records from the dataset are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of Appendix E of DCID 6/3 and ICD 503, or successor ICD.

### 2. Track 2 Information Acquisition: Search and Retention

a) *Type of Access.* NCTC may provide the owner of a dataset that contains or that may contain terrorism information with query terms – either singly or in batches – consisting of terrorism datapoints so that a search of the dataset may be run (hereinafter “Track 2” access).

b) *Standard.* Information from the dataset that is responsive to queries using NCTC-provided terrorism datapoints will be given by the data provider to NCTC. NCTC may acquire, retain, use, and disseminate information acquired under Track 2 for all authorized NCTC purposes, as described in these Guidelines. NCTC’s activities in Track 2 shall be designed solely to identify information that is reasonably believed to be terrorism information. If the information given by a data provider to NCTC does not constitute terrorism information, NCTC will promptly purge any information whose retention, use, or dissemination is not authorized by sections IV and V below.

c) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that terrorism datapoints and responsive records from the dataset are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 and ICD 503, or successor ICD.

### 3. Track 3 Information Acquisition: NCTC Dataset Acquisition

a) *Type of Access.* NCTC may acquire and replicate portions or the entirety of a dataset when necessary to identify the information that constitutes terrorism information within the dataset (hereinafter “Track 3” access).

b) *Standard and Process.* Replication of data is appropriate when the Director of NCTC, or a designee who serves as Principal Deputy Director or as a Deputy Director (hereinafter “Designee”), determines in writing, after coordination with the data provider, that a dataset is

## UNCLASSIFIED

likely to contain significant terrorism information and that NCTC's authorized purposes cannot effectively be served through Tracks 1 or 2. When making a determination, the Director or Designee also shall consider whether NCTC's authorized purposes can effectively be served by the replication of a portion of a dataset. Datasets received in accordance with Track 3 may not be accessed or used by NCTC prior to replication, except as directly necessary to make the determination above or to accomplish such replication, subject to procedures agreed upon with the data provider. Measures will be put in place to ensure that the dataset is received and stored in a manner to prevent unauthorized access and use prior to the completion of replication.

*c) Identification of United States Person Information and Temporary Retention Period.* For all datasets received pursuant to Track 3, NCTC will use reasonable measures to identify and mark or tag United States person information contained within those datasets. Any United States person information acquired pursuant to Track 3 may be retained and continually assessed for a period of up to five years by NCTC to determine whether the United States person information is reasonably believed to constitute terrorism information (hereinafter "temporary retention period"). The Terms and Conditions shall establish the temporary retention period for continual assessment of such information. The temporary retention period specified in the Terms and Conditions may be up to five years unless a shorter period is required by law, including any statute, executive order, or regulation. In no event may NCTC retain the information for longer than is permitted by law. The temporary retention period shall commence when the data is made generally available for access and use following both the determination period discussed in section III.C.3(b) immediately above, and any necessary testing and formatting. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized NCTC purposes, as described in these Guidelines.

*d) Baseline Safeguards, Procedures, and Oversight Mechanisms.* During the temporary retention period, the following baseline safeguards, procedures, and oversight mechanisms shall apply to all datasets acquired pursuant to Track 3 that have been determined to contain United States person information:

- (1) These datasets will be maintained in a secure, restricted-access repository.
- (2) Access to these datasets will be limited to those NCTC personnel who are acting under, and agree to abide by, NCTC's information sharing and use rules, including these Guidelines; who have the requisite security clearance and a need-to-know in the course of their official duties; and who have received the training required by section III.B.3.
- (3) Access to these datasets will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with rules applicable to the data for which audit records apply.

UNCLASSIFIED

(4) NCTC's queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information that is reasonably believed to constitute terrorism information. NCTC shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in Track 3 data, NCTC may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the DNI shall report these activities as required by that Act.

(5) NCTC will conduct compliance reviews as described below in section VI.

e) *Enhanced Safeguards, Procedures, and Oversight Mechanisms.* In addition to the requirements of paragraph (d), at the time when NCTC acquires a new dataset or a new portion of a dataset, the Director of NCTC or Designee shall determine, in writing, whether enhanced safeguards, procedures, and oversight mechanisms are needed. In making such a determination, the Director of NCTC or Designee shall (i) consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, and (ii) consider the sensitivity of the data; the purpose for which the data was originally collected by the data provider; the types of queries to be conducted; the means by which the information was acquired; any request or recommendation from the data provider for enhanced safeguards, procedures, or oversight mechanisms; the terms of any applicable international agreement regarding the data; the potential harm or embarrassment to a United States person that could result from improper use or disclosure of the information; practical and technical issues associated with implementing any enhanced safeguards, procedures, or oversight mechanisms; and all other relevant considerations. If the Director of NCTC or Designee determines that enhanced safeguards, procedures, and oversight mechanisms are appropriate, the determination shall include a description of the specific enhanced safeguards, procedures, or oversight mechanisms that will govern the continued retention and assessment of the dataset. These enhanced safeguards, procedures, or oversight mechanisms may include the following:

- (1) Additional procedures for review, approval, and/or auditing of any access or searches;
- (2) Additional procedures to restrict searches, access, or dissemination, such as procedures limiting the number of personnel with access or authority to search, establishing a requirement for higher-level authorization or review before or after access or search, or requiring a legal review before or after United States person identities are unmasked or disseminated;
- (3) Additional use of privacy enhancing technologies or techniques, such as techniques that allow United States person information or other sensitive information to be "discovered" without providing the content of the information, until the appropriate standard is met;

## UNCLASSIFIED

- (4) Additional access controls, including data segregation, attribute-based access, or other physical or logical access controls;
- (5) Additional, particularized training requirements for NCTC personnel given access or authority to search the dataset; and
- (6) More frequent or thorough reviews of retention policies and practices to address the privacy and civil liberties concerns raised by continued retention of the dataset.

Any enhanced safeguards, procedures, and oversight mechanisms must be included in the Terms and Conditions, or specified in writing and appended to the Terms and Conditions, and shall be kept on file as required by NCTC's record retention schedule.

f) *Removal of Information.* NCTC shall remove from NCTC's systems all identified information concerning United States persons that NCTC does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the Terms and Conditions if the Terms and Conditions specify a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section V below.

g) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that information for dataset replications is provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 and ICD 503, or successor ICD.

### IV. Dissemination

#### A. General Dissemination Requirements

1. *Definition.* For purposes of these Guidelines, dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC by any means, to include oral, electronic, or physical means.
2. *Terms and Conditions and Privacy Act.* All disseminations under these Guidelines must be: (i) compatible with any applicable Terms and Conditions or, if not compatible, the data provider must have otherwise consented to the dissemination; and (ii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.
3. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* These Guidelines are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II above). To the extent that these

## UNCLASSIFIED

Guidelines allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. § 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments.

### **B. Dissemination of United States Person Information Acquired Under Tracks 1, 2, or 3**

NCTC may disseminate United States person information properly acquired under Tracks 1, 2, or 3 if the General Dissemination Requirements are met, and if:

- (1) *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and NCTC is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity that is reasonably believed to have a need to receive such information for the performance of a lawful function;
- (2) *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting NCTC in determining whether the United States person information constitutes terrorism information. Any such recipients may only use the information for this limited purpose, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to NCTC and promptly thereafter return the information to NCTC or destroy it unless NCTC authorizes continued retention after the specific information is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines. Recipients of information under this paragraph may not retain the information for purposes of continual assessment of whether it constitutes terrorism information unless such retention would be permitted by the dissemination criteria in section IV.C.1. Any access to or dissemination under this paragraph of any bulk dataset or significant portion of a dataset believed to contain United States person information must be: (i) approved by the Director of NCTC; and (ii) expressly allowed by the Terms and Conditions or otherwise expressly approved by the data provider. In addition, the recipient of any bulk dataset or significant portion of a dataset under this provision must agree in writing that it: (i) will not disseminate the information further without prior approval by NCTC; (ii) will use the data solely for the limited purpose specified in this provision; (iii) will promptly return the data to NCTC or destroy it after providing the required assistance to NCTC, unless NCTC authorizes continued retention of specific information after it is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines; (iv) will comply with any safeguards and procedures deemed appropriate by the ODNI General Counsel and ODNI Civil Liberties Protection Officer; and (v) will

## UNCLASSIFIED

report to NCTC any significant data breach or failure to comply with the terms of its agreement. In deciding whether to approve dissemination under this paragraph of any bulk dataset or significant portion of a dataset, the Director of NCTC shall consider whether the limited purpose of this paragraph can be satisfied by allowing access to the data while it remains under NCTC's control and whether the recipient of the data has the capabilities necessary to comply with the requirements specified above;

- (3) *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or
- (4) *Dissemination of Publicly Available Information.* The United States person information is publicly available.

### **C. Dissemination of United States Person Information Acquired Under Track 3**

1. *Standard (Non-bulk) Dissemination of Specific Information Acquired Under Track 3.* In addition to the provisions above for dissemination under all three tracks, NCTC may disseminate specific United States person information acquired under Track 3 that has been handled and subsequently identified in accordance with applicable Track 3 safeguards and procedures,<sup>3</sup> if the General Dissemination Requirements are met, and if the United States person information:

- a) Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or reasonably appears to be necessary to understand or assess foreign intelligence, counterintelligence, or foreign aspects of international narcotics activities, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;
- b) Reasonably appears to be evidence of a crime, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;
- c) Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the ODNI Office of General Counsel;
- d) Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or

---

<sup>3</sup> This paragraph does not authorize NCTC to search for the additional categories of information, but rather allows NCTC to disseminate specific United States person information discovered while performing counterterrorism analysis and searches in accordance with these Guidelines and the applicable Terms and Conditions.

## UNCLASSIFIED

(ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;

e) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;

f) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;

g) Is disseminated to other recipients, if the subject of the information provides prior consent in writing;

h) Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or

i) Is disseminated to appropriate elements of the Intelligence Community for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed that it may become necessary to understand and assess such information.

**2. Bulk Dissemination of Information Acquired Under Track 3 to IC Elements.** If the General Dissemination Requirements in section IV.A above are met, NCTC also may disseminate United States person information acquired under Track 3 to other IC elements under the following conditions:

a) *General Requirements.* Any dissemination under these Guidelines of any bulk dataset or significant portion of a dataset believed to contain United States person information, which has not been assessed as constituting terrorism information, must be approved by the Director of NCTC and must be expressly allowed by the applicable Terms and Conditions for that dataset or otherwise expressly approved by the data provider. IC elements that receive or access bulk datasets or significant portions of a dataset under these Guidelines are not authorized to make further bulk disseminations of that information.

b) *Bulk Dissemination in Support of Counterterrorism Missions:* The Director of NCTC shall only approve such dissemination to IC elements in support of a legally authorized counterterrorism mission if the receiving element head agrees in writing to abide by the

## UNCLASSIFIED

provisions of the Appendix to these Guidelines and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC.<sup>4</sup> The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer, in consultation with the Assistant Attorney General for National Security, shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance.

c) *Bulk Dissemination in Support of Other Intelligence Missions:* The Director of National Intelligence shall only approve such dissemination to IC elements in support of lawful intelligence missions other than counterterrorism missions if: such dissemination is expressly allowed by the applicable Terms and Conditions; the receiving element has Attorney General-approved procedures in place for the collection, retention, and dissemination of United States person information, as required by the opening paragraph of section 2.3 of Executive Order 12333; and the receiving element head agrees in writing to abide by safeguards, procedures, and oversight mechanisms substantially similar to the safeguards, procedures, and oversight mechanisms identified in the Appendix to these Guidelines, as well as any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular datasets or otherwise required by the Director of NCTC. In addition, the Director of National Intelligence may only approve bulk dissemination to IC elements in support of intelligence missions other than counterterrorism missions if the Director of National Intelligence, in consultation with the ODNI General Counsel, determines that the proposed dissemination is necessary to a lawful mission of the IC element and that the IC element's need for the information cannot be fulfilled through dissemination of specific information under the standard dissemination provisions of section IV.C.1; through dissemination of a smaller portion of the data proposed for dissemination; or by allowing access to the data while it remains within NCTC's control. The Director of National Intelligence will provide a copy of this determination to the Assistant Attorney General for National Security. The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance. Any such agreement must be approved by the Attorney General or his delegee prior to allowing such dissemination, and the National Security Division of the Department of Justice may conduct an independent assessment of the element's oversight and compliance capabilities.

---

<sup>4</sup> If an IC element with a counterterrorism mission requests changes to provisions in the Appendix to address agency-specific circumstances (e.g., technological capabilities), such changes may be adopted if expressly approved by the data provider and by the DNI and the Attorney General or their delegees, provided that any agency-specific Appendix shall retain safeguards, procedures, and oversight mechanisms substantially similar to those contained in the original Appendix.



#### **D. Foreign Disseminations**

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section IV, NCTC must find that: (i) the dissemination is consistent with the interests of the United States, including U.S. national security interests; (ii) the dissemination complies with DCID 6/6 or any successor ICD<sup>5</sup>; (iii) the foreign or international entity agrees not to disseminate the information further without approval by NCTC; and (iv) NCTC, in consultation with ODNI General Counsel, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

#### **E. Other Disseminations**

If NCTC properly acquires any United States person information under Tracks 1 and 2 that would be authorized for dissemination pursuant to section IV.C.1 if it were acquired under Track 3, it shall consult with the data provider and advise the data provider of the existence of such information. The data provider may disseminate the information or authorize NCTC to do so.

#### **V. Retention of Information for Administrative Purposes**

To the extent consistent with law, United States person information acquired pursuant to these Guidelines may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from NCTC's systems once retention is no longer necessary or required for those purposes, except that NCTC may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

#### **VI. Compliance**

##### **A. Periodic Compliance Reviews**

Subject to oversight by the ODNI Civil Liberties Protection Officer, NCTC shall conduct periodic reviews to verify continued compliance with these Guidelines, including compliance with the Terms and Conditions, and with all baseline and enhanced safeguards, procedures, and oversight mechanisms. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

---

<sup>5</sup> ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing ICPGs and IC Standards.

**B. Periodic Reviews of the Need for Continued Assessment**

NCTC, in coordination with the ODNI Civil Liberties Protection Officer, shall conduct periodic reviews of all datasets replicated under Track 3 to determine whether retention and continued assessment of the United States person information in those datasets remains appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was acquired, the success of that dataset in fulfilling legitimate counterterrorism purposes, whether those purposes can now be fulfilled through Track 1 or 2 access to the dataset, through the use of other datasets in NCTC's possession, or through other appropriate means, and privacy and civil liberties considerations applicable to the particular dataset. NCTC shall also conduct periodic reviews of the continued necessity and efficacy of bulk disseminations permitted under the Guidelines. NCTC shall report the results of these periodic reviews to the IC Inspector General.

**C. NCTC's Computer Systems**

In designing its computer systems, NCTC shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, these Guidelines.

**D. Reporting**

1. NCTC shall promptly report, in writing, to the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with: (i) these Guidelines; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions. For the purposes of these Guidelines, a "significant failure" is a failure that constitutes a violation of the Constitution or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

2. The Director of NCTC shall report annually in writing to the ODNI Civil Liberties Protection Officer on the measures that NCTC is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under these Guidelines and in compliance with the baseline and enhanced safeguards, procedures, and oversight mechanisms, and all applicable Terms and Conditions. The report shall include:

- (1) For datasets replicated under Track 3, the results of the review required in section VI.B above, regarding whether replication continues to be appropriate;
- (2) A general description of NCTC's compliance and audit processes;

## UNCLASSIFIED

(3) A description of the audits, spot checks, and other reviews NCTC conducted during the previous year, and the results of those audits, spot checks, or other reviews, to include any shortcomings identified;

(4) A description of how NCTC ensures that it promptly purges United States person information that does not meet the standards for retention under these Guidelines;

(5) An assessment of United States person information disseminated by NCTC directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that NCTC imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section IV.B.2;

(6) A description of any approvals by the DNI or Director of NCTC, in accordance with sections IV.B.2 and IV.C.2 above, to provide access to or to disseminate bulk datasets or significant portions of a dataset;

(7) An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or whether any other reasonable measures that should be taken to improve the handling of information;

(8) A description of measures that NCTC has taken to comply with the requirements of section VI.C with respect to its data processing systems; and

(9) A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines.

3. NCTC shall provide a copy of this report to the ODNI General Counsel and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. NCTC shall also make available to the IC Inspector General any other reports or documentation necessary to ensure compliance with these Guidelines.

4. The reporting required by these Guidelines does not replace any other reporting required by statute, executive order, or regulation.

### **E. Privacy and Civil Liberties Oversight Board**

Pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Privacy and Civil Liberties Oversight Board shall have access to all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other material that it deems relevant to its oversight of NCTC activities.

## UNCLASSIFIED

### **VII. Interpretation and Departures**

A. NCTC shall refer all questions relating to the interpretation of these Guidelines to the ODNI Office of General Counsel. The ODNI General Counsel shall consult with the Assistant Attorney General for National Security regarding any novel or significant interpretations.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve any departures from these Guidelines. If there is not time for such approval and a departure from these Guidelines is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director of NCTC or the Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

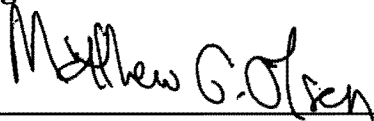
### **VIII. Status as Internal Guidance**

These Guidelines are set forth solely for the purpose of internal NCTC and ODNI guidance. They are not intended to, and do not, create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, agents, or any other person, nor do they place any limitation on otherwise lawful investigative or litigation prerogatives of the United States.

### **IX. Revocations, Transitions, and Effective Date.**

These Guidelines supersede and revoke the Memorandum of Agreement signed by the Director of National Intelligence and Attorney General on October 1, 2008 and November 4, 2008, respectively, along with any amendments to that Agreement. Terms and Conditions entered pursuant to that Memorandum of Agreement, or similar information sharing agreements to which NCTC is currently a party, remain in effect until revoked or until amended or replaced consistent with these Guidelines. As applied to NCTC, these Guidelines also supersede NCTC's EO 12333, § 2.3 Procedures with respect to the data and datasets covered by these Guidelines. These Guidelines shall be effective upon the approval of the Attorney General, the Director of National Intelligence, and the Director of NCTC.

Signed



Matthew G. Olsen  
Director, National Counterterrorism Center

MAR 21 2012

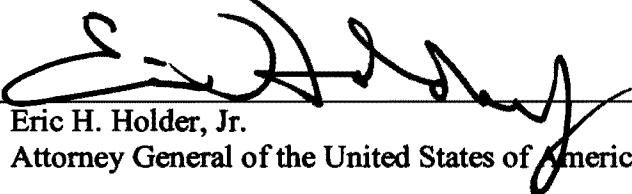
Date



James R. Clapper, Jr.  
Director of National Intelligence

21 MAR 2012

Date



Eric H. Holder, Jr.  
Attorney General of the United States of America

3 - 22 - 12

Date

# UNCLASSIFIED

## Appendix

### **Safeguards, Procedures, and Oversight Mechanisms for Bulk Dissemination of Information Acquired Under Track 3 to IC Elements**

#### **I. Purpose**

This Appendix contains the safeguards, procedures, and oversight mechanisms that an Intelligence Community (IC) element head, or designee, must agree to, in writing, before NCTC may disseminate any bulk dataset or significant portion of a dataset (hereinafter referred to in this Appendix as “a dataset” or “data”) that includes United States Person information in accordance with section IV.C.2(b) of the NCTC Guidelines. NCTC may only disseminate datasets under this Appendix in support of the receiving IC element’s legally authorized counterterrorism mission.

#### **II. Implementation**

Prior to NCTC’s dissemination of any bulk dataset to an IC element, the element head must agree in writing to abide by the provisions of this Appendix, and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC (hereinafter “written agreement”). All requirements shall be described, referenced, or appended to the written agreement, which the Director of NCTC shall develop in consultation with the ODNI General Counsel and Civil Liberties Protection Officer. If an IC element is provided access to NCTC’s systems in support of its legally authorized counterterrorism mission and NCTC will undertake any of the requirements in this Appendix on behalf of the IC element, the IC element head and the Director of NCTC shall specify in the written agreement the persons, by name or position, responsible for all training, oversight, and related compliance measures and reporting.

#### **III. Definitions**

For the purposes of this Appendix, the following definitions apply:

- A. Dissemination:** Dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC and/or the IC element by any means, to include oral, electronic, or physical means.
- B. IC Element:** The term “IC element” refers to the specific IC element that is provided data in accordance with section IV.C.2(b) of the NCTC Guidelines in support of the IC element’s legally authorized counterterrorism mission.
- C. Terrorism Information:** The term “terrorism information”—
  - (1) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

UNCLASSIFIED

## UNCLASSIFIED

- (i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
  - (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
  - (iii) communications of or by such groups or individuals; or
  - (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
- (2) includes weapons of mass destruction information. 6 U.S.C. § 485(a)(5).

**D. United States Person.** For an IC element receiving information under this Appendix, this term has the meaning given the term in that element's guidelines approved by the Attorney General under section 2.3 of Executive Order 12333. For an element without such Attorney General-approved guidelines, or whose guidelines do not contain such a definition, this term means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States 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. *See* Executive Order 12333 § 3.5(k).

#### IV. General Provisions

**A. Authorized Purpose.** The IC element may access and acquire United States person information in the dataset for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,<sup>1</sup> used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures in this Appendix, the applicable Terms and Conditions for that dataset, and any other measures specified in the written agreement. Information is "reasonably believed to constitute terrorism information" if, based on the knowledge and experience of counterterrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information.

**B. Erroneously Provided Information and Errors in Information.** Any United States person information that has been erroneously disseminated to the IC element will not be retained, used, or further disseminated by the IC element. Such information will be promptly removed from the IC element's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the

---

<sup>1</sup> For purposes of this Appendix, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with the IC element's records retention policies.

## UNCLASSIFIED

Attorney General. Information in the IC element's systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and NCTC shall be notified of the error promptly.

**C. Removal of Information.** The IC element shall remove from the IC element's systems all identified information concerning United States persons that the IC element does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the written agreement if it specifies a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section VII below.

**D. Training.** The IC element shall ensure that all employees and contractors of the IC element and detailees and assignees to the IC element from other agencies (hereinafter "IC element personnel") provided access to the data under this Appendix will receive training in the use of each dataset to which they will have access to ensure that they use the data only for the IC element's authorized counterterrorism purposes and in accordance with this Appendix and other applicable requirements. The training shall also ensure that they understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each dataset. This training shall be in person, whenever practical, and refreshed at least annually. IC element personnel provided access to data under this Appendix will also receive ongoing training to ensure understanding of this Appendix and other applicable agreements and the civil liberties and privacy expectations and requirements involved in the access to and use of the data.

**E. Authorized Uses of Information and Time Periods.** For all datasets or data received pursuant to this Appendix, the IC element will use reasonable measures to identify and mark or tag United States person information contained within those datasets (to the extent not already done so by the data provider and NCTC). Any United States person information accessed or acquired in accordance with this Appendix may be continually assessed for up to five years by IC element personnel to determine whether the United States person information is reasonably believed to constitute terrorism information unless a shorter temporary retention period is specified in the written agreement with NCTC. The written agreement signed by the IC element head or designee shall specify the applicable temporary retention period for the dataset or data as required by the Terms and Conditions or otherwise required by the Director of NCTC. The temporary retention period shall commence when the data is made generally available for access and use by NCTC; the period is not restarted at the time of dissemination to or access by the IC element. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized IC element purposes. These include, but are not limited to: analysis and integration purposes, inclusion in finished analytic products and pieces,



## UNCLASSIFIED

enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support and planning, and appropriate dissemination to Intelligence Community elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth below. Any additional protections or provisions required by the Terms and Conditions for that dataset or otherwise required by the Director of NCTC must be included in the written agreement signed by the IC element head or designee.

**F. Applicable Laws and Policies.** The IC element shall access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. This Appendix does not apply to information whose retention, use, and dissemination is governed by court order or court-approved procedures. If the IC element has Attorney General-approved procedures pursuant to section 2.3 of Executive Order 12333, those are hereby superseded as applied to the collection, retention, and dissemination of United States person information in data and datasets governed by this Appendix, except as otherwise specifically provided herein.

**G. Limitation.** The IC element shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. IC element personnel who access NCTC's databases will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, and to additional audit and oversight requirements, as applicable and as specified in the written agreement signed by the IC element head or designee. IC elements may be required to adopt or apply similar role-based access and information sharing policies prior to receiving and storing data from NCTC; any such requirements will be specified in the written agreement signed by the IC element head or designee.

**H. Information Access Requests.** For information governed by this Appendix, it shall be the responsibility of the data provider who provided the data to NCTC to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement was agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and as specified in the Terms and Conditions for that information.

**I. Baseline Safeguards, Procedures, and Oversight Mechanisms.** During the temporary retention period, the IC element shall adhere to the following baseline

## UNCLASSIFIED

safeguards, procedures, and oversight mechanisms for any dataset disseminated by NCTC under this Appendix:

1. The data will be maintained in a secure, restricted-access repository.
2. Access to the data will be limited to those IC element personnel, who: (i) access the data for the purpose authorized in section IV.A; (ii) are acting under, and agree to abide by, the IC element's information sharing and use rules, including this Appendix and the written agreement; (iii) have the requisite security clearance and a need-to-know in the course of their official duties; and (iv) have received the training required by section IV.D.
3. Access to the data will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with the rules applicable to the data for which audit records apply.
4. The IC element's queries or other activities to assess information contained in the data disseminated pursuant to this Appendix shall be designed solely to identify information that is reasonably believed to constitute terrorism information.
5. The IC element shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in data disseminated pursuant to this Appendix, the IC element may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, which are known or suspected terrorist identifiers or other pieces of terrorism information, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the IC element shall coordinate with NCTC to ensure proper reporting and to identify which element should report these activities as required by that Act.
6. The IC element will conduct compliance reviews as described below in section IX.

**J. Enhanced Safeguards, Procedures, and Oversight Mechanisms.** The IC element must also comply with any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by

UNCLASSIFIED

the Director of NCTC and specified in the written agreement signed by the IC element head or designee. See NCTC Guidelines, section III.C.3(e).

**V. Dissemination of United States Person Information**

**A. General Dissemination Requirements.**

1. *Terms and Conditions and Privacy Act.* All disseminations under this Appendix must be: (i) compatible with this Appendix; (ii) any applicable Terms and Conditions, and any other measures identified or specified in the written agreement or, if not compatible, the data provider must have otherwise consented to the dissemination; and (iii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.

2. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* The NCTC Guidelines and this Appendix are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II of the NCTC Guidelines). To the extent that the NCTC Guidelines, this Appendix, and the written agreement allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments. This Appendix is not intended to, does not, and shall not be relied upon to create a grant of new or additional authority for information sharing with or dissemination of information to state, local, or tribal authorities or private-sector entities.

3. *Bulk Disseminations Prohibited.* In no case may the IC element make a further bulk dissemination of any dataset or any significant portion of a dataset. However, specific United States person information may be disseminated pursuant to the dissemination provisions in sections V.B or V.C below.

**B. Basic Dissemination Requirements.** The IC element may disseminate United States person information from datasets provided by NCTC if the General Dissemination Requirements are met, and if:

1. *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and the IC element is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity or individual, that is

## UNCLASSIFIED

reasonably believed to have a need to receive such information for the performance of a lawful function;

2. *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting the IC element in determining whether the United States person information constitutes terrorism information. Before disseminating information under this paragraph, the IC element should consider approaching NCTC for this type of assistance. Any such recipients may only use the information for the limited purpose identified in this paragraph, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to the IC element and promptly thereafter return the information to the IC element or destroy it unless the IC element authorizes continued retention after the specific information continued retention after the specific information is determined by the IC element to meet the dissemination criteria in section V.C of this Appendix. Recipients of information under this paragraph may not retain the information for continual assessment of whether it constitutes terrorism information unless such retention is permitted by the dissemination criteria in section V.C of this Appendix. This paragraph does not authorize the IC element to disseminate any bulk dataset or significant portion of a dataset believed to contain United States person information;

3. *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or

4. *Dissemination of Publicly Available Information.* The United States person information is publicly available.

**C. Dissemination of Non-Terrorism Information.** In addition, the IC element may disseminate United States person information contained in datasets provided by NCTC if that United States person information has been handled and subsequently identified in accordance with applicable safeguards and procedures,<sup>2</sup> if the General Dissemination Requirements are met, and if the United States person information:

1. Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or

---

<sup>2</sup> Note that this dissemination category does not authorize the IC element to search for additional categories of information, but rather allows the IC element to disseminate certain United States person information uncovered while performing counterterrorism analysis and searches in accordance with this Appendix, the applicable Terms and Conditions, and the written agreement.

## UNCLASSIFIED

reasonably appears to be necessary to understand or assess foreign intelligence or counterintelligence or foreign aspects of international narcotics activities, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;

2. Reasonably appears to be evidence of a crime, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;

3. Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the IC element's Office of General Counsel or senior legal advisor;

4. Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or (ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;

5. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;

6. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;

7. Is disseminated to other recipients, if the subject of the information provides prior consent in writing;

8. Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or

9. Is disseminated to appropriate elements of the IC for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

## UNCLASSIFIED

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed it may become necessary to understand and assess such United States person information described above.

### **VI. Foreign Disseminations**

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section V, the IC element must find that:

- A. the dissemination is consistent with the interests of the United States, including U.S. national security interests;
- B. the dissemination complies with DCID 6/6 or any successor ICD<sup>3</sup>;
- C. the foreign or international entity has agreed not to disseminate the information further without approval by the IC element; and
- D. the IC element, in consultation with its General Counsel or senior legal advisor, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

### **VII. Retention of Information for Administrative Purposes**

To the extent consistent with law, United States person information acquired pursuant to this Appendix may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from the IC element's systems once retention is no longer necessary or required for those purposes, except that the IC element may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

### **VIII. The IC Element's Computer Systems**

In designing its computer systems, the IC element shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, this Appendix.

---

<sup>3</sup> ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing IC Policy Guidance and IC Standards.

**IX. Oversight and Compliance**

A. Subject to oversight by the IC element's Civil Liberties and/or Privacy Officer, if applicable, and the ODNI Civil Liberties Protection Officer, the IC element shall conduct periodic reviews to verify continued compliance with this Appendix, including compliance with any Terms and Conditions and any measures specified in the written agreement. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

B. The IC element, in coordination with the IC element's Civil Liberties and/or Privacy Officer (or other appropriate official as identified in the written agreement), shall conduct periodic reviews of its continued need for access to each dataset disseminated pursuant to the NCTC Guidelines and this Appendix to determine whether such access remains necessary and appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was disseminated; the success of that dataset in fulfilling legitimate counterterrorism purposes; whether those purposes can now be fulfilled through the use of other data in the IC element's possession, or through other appropriate means; and privacy and civil liberties considerations applicable to the particular dataset.

C. The IC element shall promptly report, in writing, to the IC element head, the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with (i) this Appendix; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions or the written agreement. For the purposes of this Appendix, a "significant failure" is a failure that constitutes a violation of the Constitution, or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall then report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

D. The IC element shall report annually in writing to the IC element head and to the ODNI Civil Liberties Protection Officer on the measures that the IC element is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under this Appendix, and in compliance with all Terms and Conditions and written agreement. The report shall include:

1. The results of the review required in section IX.B. above, regarding whether access to the bulk dataset continues to be appropriate;
2. A general description of the IC element's compliance and audit processes;

## UNCLASSIFIED

3. A description of the audits, spot checks, and other reviews the IC element conducted during the previous year, and the results of those audits, spot checks or other reviews, to include any shortcomings identified;
4. A description of how the IC element ensures that it promptly purges United States person information that does not meet the standards for retention under this Appendix, related Terms and Conditions, and any other measures specified in the written agreement;
5. An assessment of the United States person information disseminated by the IC element directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that the IC element imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section VI.C of this Appendix;
6. An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or any other reasonable measures that should be taken to improve the handling of information;
7. Measures the IC element has taken to comply with the requirements of section VIII with respect to its computer systems; and
8. A description of any material changes or improvements the IC element implemented, or is considering implementing, to improve compliance with this Appendix.

E. The IC element shall provide a copy of this report to the IC element General Counsel, the IC element Civil Liberties and/or Privacy Officer, the Director of NCTC, the ODNI General Counsel, the IC element's Inspector General, and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. The IC element shall also make available to the IC element's Inspector General and the IC Inspector General any other reports or documentation necessary to ensure compliance with this Appendix.

F. The reporting required by this Appendix does not replace any other reporting required by statute, executive order, or regulation.

### **X. Interpretation and Departures**

A. The IC element shall refer all questions relating to the interpretation of these Guidelines to the IC element's Office of General Counsel or other senior legal advisor. The IC element's General Counsel shall consult with the ODNI General Counsel regarding any novel or significant interpretations, and the ODNI General Counsel shall



UNCLASSIFIED

then consult with the Assistant Attorney General for National Security to the extent required by the NCTC Guidelines.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve in advance any departures from this Appendix. If there is not time for such approval and a departure from this Appendix is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the IC element head, other senior IC element personnel identified in the written agreement with NCTC, the Director of NCTC, or the NCTC Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

**XI. Status as Internal Guidance**

The provisions in this Appendix are set forth solely for the purpose of internal IC element and ODNI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law or in equity, by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigation prerogatives of the U.S. Government.

**EXHIBIT O**



# The Biggest New Spying Program You've Probably Never Heard Of

July 30, 2012

*Update: Since this piece was posted, the ACLU has filed FOIA requests seeking more information on data-mining by the NCTC. [Read more »](#)*

What if a government spy agency had power to copy and data mine information about ordinary Americans from any government database? This could include records from law enforcement investigations, health information, employment history, travel and student records. Literally anything the government collects would be fair game, and the original agency in charge of protecting the privacy of those records would have little say over whether this happened, or what the spy agency did with the information afterward. What if that spy agency could add commercial information, anything it – or any other federal agency – could buy from the [huge data aggregators](#) that are monitoring our every move?

What if it wasn't just collection but also sharing? Anything that was reasonably believed to be necessary to "protect the safety or security of persons, property or organizations" or "protect against or prevent a crime or threat to national security" could be shared. Imagine the dissemination was essentially unlimited, not just to federal, state, local or foreign governments but also to individuals or entities that are not part of the government.

It has already happened.

This full frontal assault on our privacy wasn't passed through an Act of Congress or international treaty but through deceptively titled "guidelines" to the National Counterterrorism Center (NCTC). On March 22, 2012 the Attorney General, the Director of National Intelligence (DNI) and the Director of NCTC [issued an update](#) to the 2008 rules for handling information on US persons. These were radical changes (to see how different please check out [redline comparison](#) we did between the 2008 and 2012 guidelines).

The biggest change regards the NCTC's handling of "non-terrorism" related information on US persons. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or part of an actual investigation. When the NCTC gobbled up huge data sets it had to search for and identify any innocent US person information inadvertently collected, and [discard it within 180 days](#). This crucial check meant that NCTC was dissuaded from collecting large databases filled with information on innocent Americans, because the data had to then be carefully screened. The 2012 guidelines eliminate this check, allowing NCTC to collect and "continually assess" information on innocent Americans for up to five years.

Once information is acquired, the new guidelines authorize broad new search powers. As long NCTC says its search is aimed at identifying terrorism information, it may conduct queries that involve non-terrorism data points and pattern-based searches and analysis (data mining). The breadth and wrongheadedness of these changes are particularly noteworthy. Not only do they mean that anytime you interact with any government agency you essentially enter a lineup as a potential terrorist, they also rely on a technique, datamining, which has been thoroughly discredited as a useful tool for identifying terrorists. As far back as 2008 the [National Academy of Sciences found](#) that data mining for terrorism was scientifically "not feasible" as a methodology, and likely to have significant negative impacts on privacy and civil liberties.

Perhaps most disturbing, once information is gathered (not necessarily connected to terrorism), in many cases it can be shared with "a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government" – literally anyone. That sharing can happen in relation to national security and

safety, drug investigations, if it's evidence of a crime or to evaluate sources or contacts. This boundless sharing is broad enough to encompass disclosures to an employer or landlord about someone who NCTC may think is potentially a criminal, or at the request of local law enforcement for vetting an informant.

All of this is happening with very little oversight. Controls over the NCTC are mostly internal to the DNI's office, and important oversight bodies such as Congress and the President's Intelligence Oversight Board aren't notified even of "significant" failures to comply with the Guidelines. Fundamental legal protections are being sidestepped. For example, under the new guidelines, Privacy Act notices (legal requirements to describe how databases are used) must be completed by the agency that collected the information. This is in spite of the fact that those agencies have no idea what NCTC is actually doing with the information once it collects it.

All of this amounts to a [reboot of the Total Information Awareness Program](#) that Americans rejected so vigorously right after 9/11. While some outlets like the [Washington Post](#) and New York Times and bloggers such as [emptywheel](#) have written excellent pieces about these changes, due to their complexity and obscurity they haven't gotten nearly the attention they deserve.

Tomorrow I'm [testifying before Congress](#) about the general weakening of American privacy laws and how they've been specifically exploited by NCTC. We hope it will be the beginning of a process to shield innocent Americans from becoming the subject of investigations by the intelligence community. We'll be pushing for oversight hearings and additional information to evaluating the legal of the entire program.

[Here](#) is a simple guide to the main changes created by the 2012 NCTC guidelines.

*Learn more about government surveillance: [Sign up for breaking news alerts](#), [follow us on Twitter](#), and [like us on Facebook](#).*

---

Published on *American Civil Liberties Union* (<http://www.aclu.org>)

**Source URL:** <http://www.aclu.org/blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard>



---

# Government Extends Time it Can Retain Info on Innocent Americans in Counterterrorism Databases

**March 23, 2012**

The Obama administration [has extended](#) the time the National Counterterrorism Center (NCTC) can collect and hold on to records on U.S. citizens and residents from 180 days to five years, even where those people have no suspected ties to terrorism. The [new NCTC guidelines](#), which were approved by Attorney General Eric Holder, will give the intelligence community much broader access to information about Americans retained in various government databases.

The decades-old rules limiting the collection and retention of U.S. citizen and resident information by the intelligence community and the military existed for a very good reason: to ensure that the powerful tools designed to protect us from foreign enemies are not turned against Americans. Authorizing the "temporary" retention of nonterrorism-related citizen and resident information for five years essentially removes the restraint against wholesale collection of our personal information by the government, and puts all Americans at risk of unjustified scrutiny. Such unfettered collection risks reviving the Bush administration's [Total Information Awareness program](#), which Congress killed in 2003.

The previous obligation to "promptly review" data and purge nonterrorism-related U.S. citizen and resident information served to protect Americans' privacy and security by forcing the intelligence community to properly focus its collection efforts, and by compelling them to make timely reviews of information gathered. After too many intelligence failures, we've found the important pieces of information were lost in the vast streams of data collected. Making the haystack bigger will only make it harder to find the needle, endangering both privacy and security.

American citizens and residents should not be considered potential terrorists until the NCTC decides otherwise. Having innocent people's information in intelligence databases for five years without any suspicion of wrongdoing creates an unacceptable risk to Americans' privacy through error and abuse.

*Learn more about government surveillance: [Sign up for breaking news alerts](#), [follow us on Twitter](#), and [like us on Facebook](#).*

---

Published on *American Civil Liberties Union* (<http://www.aclu.org>)

**Source URL:** <http://www.aclu.org/blog/national-security/government-extends-time-it-can-retain-info-innocent-americans>



---

# Step One in Data-Mining America: Build a Big Database

**August 1, 2012**

A few days ago, [we highlighted](#) the drastic privacy implications of new guidelines issued to govern data-mining by the National Counterterrorism Center (“NCTC”). Yesterday, we testified to Congress about the problems with the guidelines, and we filed three Freedom of Information Act (“FOIA”) requests to learn more about how the guidelines will affect the privacy of millions of Americans.

As we explained before, under [the new guidelines approved by the Attorney General](#), the NCTC may aggregate federal databases consisting mainly of information about Americans with no connection to terrorism and then analyze those databases and disseminate the results for reasons also unrelated to terrorism. What databases will NCTC aggregate? We don’t know yet, but in our FOIA requests we’ve asked for details. What we do know is that the federal government collects an enormous amount of personal information for myriad reasons. Think about your healthcare services, business licenses, gun permits, welfare benefits, voting registrations, and employment records.

Under the new guidelines, the NCTC could potentially combine all the databases that store that sensitive and private information into a single, massive searchable and data-minable database.

The guidelines accomplished this sweeping transformation of the NCTC’s data-mining abilities primarily by allowing the NCTC to intentionally collect data on U.S. citizens and residents even where those people have no suspected ties to terrorism, and to keep that data for 5 years (up from 180 days).

Hidden by the dry technical details of the new guidelines is what we called a “reboot of the Total Information Awareness Program” roundly rejected by Americans after 9/11. Here is how my colleague, Chris Calabrese, described one of the main problems with the guidelines in his written statement to Congress:

In what is perhaps the most significant change, the Obama administration has extended the authority of the NCTC to intentionally collect, retain and assess data on U.S. citizens and residents, even where those people have no suspected ties to terrorism. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or related to an actual investigation. Therefore, when NCTC collected information from federal government databases, it had to search for and identify any innocent US person information inadvertently collected, and discard it within 180 days. This crucial purpose limitation meant that NCTC was dissuaded from collecting or maintaining information on innocent Americans in its large databases, and prohibited from using or disseminating it. The 2012 guidelines eliminate this check, allowing NCTC to collect and “continually assess” information on innocent Americans for up to five years.

Chris went on to describe the NCTC’s alarming new powers under the guidelines to mine the data it has aggregated:

Once NCTC acquires this information, the new guidelines give it broad new powers to search through it. As long as queries are designed to solely identify information that is reasonably believed to constitute terrorism information, it may conduct queries that involve non-terrorism data points and pattern based searches and analysis (data mining). It is particularly noteworthy that NCTC relies on a technique, data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be

caught up in terrorism investigations if this technique is utilized. As far back as 2008 the National Academy of Sciences found that data mining for terrorism was scientifically “not feasible” as a methodology, and likely to have significant negative impacts on privacy and civil liberties.

You can read Chris’s full statement to Congress [here](#).

The [three FOIA requests we filed yesterday](#) seek more information about the government’s claimed need for the updated NCTC guidelines and the likely impact on the privacy of millions of innocent U.S. citizens and residents whose private information is routinely collected in federal databases. We’ll keep you posted on how the government responds.

*Learn more about government surveillance: [Sign up for breaking news alerts](#), [follow us on Twitter](#), and [like us on Facebook](#).*

---

Published on *American Civil Liberties Union* (<http://www.aclu.org>)

**Source URL:** <http://www.aclu.org/blog/national-security-technology-and-liberty/step-one-data-mining-america-build-big-database>



Statement of Christopher R. Calabrese, Legislative Counsel

American Civil Liberties Union

Washington Legislative Office

On

State Of Federal Privacy and Data Security Law: Lagging Behind the Times?

Before the Senate Committee on Homeland Security and Governmental Affairs  
Subcommittee on Oversight of Government Management, the Federal Workforce,  
and the District of Columbia

July 31, 2012



Good morning Chairman Akaka, Ranking Member Johnson, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the importance of updating the Privacy Act and assuring accountability and oversight regarding how the federal government handles personal information.

## I. Introduction

The Privacy Act of 1974 was a landmark statute that has provided significant privacy protections but now needs to be updated. The Act formed the foundation for information privacy law, not just in the United States but around the world. The principles it delineates – the Fair Information Practices – have been written into law in almost every industrialized nation. They are the baseline best practices for anyone who gathers personal information – including governments and corporations. The practices require transparent descriptions of the information collected and grant the data subject control over how information is used and shared.<sup>1</sup>

The Privacy Act translates the fair information practices into a series of federal agency responsibilities and rights for individual citizens. Specifically, the Act controls when records can be collected and when and how they can be disclosed; allows individuals to access and correct their own records; and requires agencies to notify people about these systems and keep secure, accurate records.

However, even with this strong foundation, significant challenges have arisen in protecting personal privacy in the United States, including the data held by federal agencies. Some of these challenges arise from the age of the Privacy Act. Congress has not kept the Act up to date with existing technologies and new methods of disclosures such as data breach notification. Other challenges come from agency efforts to circumvent the Act through common practices such as boilerplate notices and the widespread use of commercial information. Still others arise from new court decisions that limit the recovery of damages under the Act.

Many of these problems are highlighted by the National Counterterrorism Center's (NCTC) recent decision claiming wide ranging authority to collect and use the personal, non-terrorist, information of innocent Americans for counterterrorism and law enforcement investigations.

This testimony is divided into four parts:

1. Updates to the Privacy Act;
2. Federal data breach notification;
3. Privacy Act remedies and oversight; and

---

<sup>1</sup> The full description of these principles can be found here: OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980).

4. Increased use of non-terrorism related information by the National Counterterrorism Center

I will discuss each of these problems in turn and provide recommendations to eliminate or mitigate them.

## II. Updates to the Privacy Act

In 2008, this committee held a hearing, *Protecting Personal Information: Is the Federal Government Doing Enough?*, which explored many of the longstanding problems with the Privacy Act. Specifically, the testimony of Ari Schwartz from the Center for Democracy and Technology described several problems with the Privacy Act and privacy protections across federal agencies.<sup>2</sup> These issues have also been the focus of numerous studies by the US Government Accountability Office (GAO).<sup>3</sup> Longstanding issues include:

- the limited definition of “system of records”,
- overuse of the “routine use” exception,
- failure to extend the protections of the Privacy Act to the government’s use of commercial databases,
- shortcomings in agency compliance with the requirements of the E-Government Act of 2002 in regard to promulgating Privacy Impact Assessments, and
- the lack of privacy leadership at the Office of Management and Budget (OMB) and in some agencies.

Each of these problems persists four years later. I expect other members of the distinguished panel to describe them in detail. Rather than duplicate those efforts I will briefly highlight some key areas of focus.

*System of records.* The Privacy Act regulates “systems of records” and anything that falls outside of that scope is not regulated by the Act.<sup>4</sup> Unfortunately, this definition is unduly restrictive because it is tied to the process of retrieving information about a specific individual or information tied to that individual. Current technologies allow for a variety of search techniques using a range of criteria that are not tied to an individual. In discussing this problem, the GAO has noted “a data-mining system that performs analysis by looking for patterns in personal

---

<sup>2</sup> *Protecting Personal Information: Is the Federal Government Doing Enough?*: Hearing before the S Committee on Homeland Security and Governmental Affairs, 110<sup>th</sup> Cong. (2008) (Statement of Ari Schwartz, Vice President, Center for Democracy & Technology) available at: <http://www.hsgac.senate.gov/hearings/protecting-personal-information-is-the-federal-government-doing-enough>

<sup>3</sup> GAO, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* GAO-08-795T (Washington D.C.: Jun 18, 2008); GAO, *Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603, (Washington D.C.: May 30, 2008).

<sup>4</sup> System of records is defined as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual” 5 U.S.C. 552a(a)(5).

information located in other systems of records or that performs subject-based queries across multiple data sources may not constitute a system of records under the act.”<sup>5</sup>

*Routine Use.* The routine use exception to the Privacy Act’s disclosure provisions allows agencies to disclose information from systems of records without first obtaining consent from the individuals whose privacy is impacted. Although Congress intended this exception to permit records sharing only when “proper and necessary,”<sup>6</sup> the exception has become a catchall used to justify a wide array of disclosures. Seemingly, agencies are bound only by what they publish in the Federal Register as a routine use. The statutory requirement that disclosures be “compatible with the purpose for which [the information] was collected”<sup>7</sup> has been largely ignored. Thus, in practice, the routine use exception serves to circumvent the purpose of the Privacy Act by allowing disclosures at an agency’s whim.

*Commercial Databases.* The Privacy Act does not extend to the federal government’s use of commercial databases, despite the fact that such use has become widespread and prolific.<sup>8</sup> These databases frequently contain incorrect information and offer few of the protections, such as access, notice, correction and purpose limitations, which are fundamental to the Privacy Act and fair information practices. In spite of these shortcomings, commercial databases are often accessed for a wide variety of purposes by law enforcement and other agencies, including as part of background check investigations.<sup>9</sup>

*Privacy Act Notifications.* While agencies have made improvements in providing Privacy Impact Assessments (PIA) and System of Record Act Notices (SORN) for their databases, these notifications are frequently hard to find and often consist of boilerplate language which does a poor job of describing the actual uses of the database and how they handle personal information.<sup>10</sup> This information is sometimes scattered across agency websites and is difficult to find and understand.

*Agency Leadership on Privacy.* Since 2005 when agency privacy officers’ authority was expanded and formalized, agencies have made strides in adding expertise and leadership on privacy.<sup>11</sup> However, in too many agencies, the title of Chief Privacy Officer is held by a senior agency level official such as the Chief Information Officer or General Counsel, but the actual

---

<sup>5</sup> GAO-08-795T, page 15.

<sup>6</sup> LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 967 (Joint Comm. on Gov’t Operations ed., 1976) available at [http://www.loc.gov/rr/frd/Military\\_Law/pdf/LH\\_privacy\\_act-1974.pdf](http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf).

<sup>7</sup> 5 U.S.C. § 552(a)(a)(7).

<sup>8</sup> See for example GAO, *Privacy: Government Use of Data From Information Resellers Could Include Better Protections*, GAO-08-543T (Washington D.C.: March 11, 2008).

<sup>9</sup> For more please see the ACLU statement on regulation of data aggregators: <http://www.aclu.org/technology-and-liberty/letter-support-s-1490-personal-data-privacy-and-security-act>

<sup>10</sup> United States. White House. Office of Management and Budget. *Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. Washington: GPO, 2012.

<sup>11</sup> 42 USC 2000ee-1.

privacy related responsibilities are handled by a much lower ranking official. Similarly, in spite of OMB's wide ranging responsibilities over privacy, the agency maintains no central privacy officer. These deficiencies result in fragmentation of the responsibility for maintaining privacy protections and uneven compliance with privacy related statutes and regulations.<sup>12</sup>

**Recommendation:** Each of these important and longstanding problems would be addressed in significant part by S.1732, Privacy Act Modernization for the Information Age Act of 2011. The ACLU believes passage of the portions of this legislation addressing these issues would be an important step forward in updating the Act and improving privacy in federal agencies.

### III. Federal data breach notification

Breaches of data are an ongoing and serious problem. According to records compiled by Privacy Rights Clearinghouse, since 2008 at least 78 breaches of information held by federal agencies have occurred, compromising at least 77 million records.<sup>13</sup> However, existing OMB guidance on data breaches at federal agencies is inadequate and leaves too much discretion to individual agencies in determining whether to disclose breaches.

Relying on the Privacy Act as well as federal data privacy laws, the OMB memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (M-07-16) directs federal agencies to implement a data breach notification policy by September 22, 2007 and outlines the framework for doing so.<sup>14</sup> The memorandum is split into four parts, each titled "attachment," which cover the treatment of personally identifiable information (PII), security requirements, outside notification in cases of a breach, and consequence of failures in agency compliance. This guidance only applies to federal executive agencies.

There is significant room for improvement in this guidance. On the positive side, it is mandatory for all agencies, requires basic security protections such as encryption, and advocates that agencies adopt privacy best practices such as data minimization and access limitations. It also prescribes a review of existing databases to assure that their contents are still relevant and necessary and requires the elimination of unnecessary uses of social security numbers. These requirements are particularly important for controlling sensitive information and reducing identity theft.

Where major problems arise with the guidance is in its recommendations for when affected individuals should be notified in the event of a data breach. In contrast to many state

---

<sup>12</sup> GAO, *Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions*, GAO-08-603 (Washington D.C.: May 2008).

<sup>13</sup> *Chronology of Data Breaches*, Privacy Rights Clearing House, <http://www.privacyrights.org/data-breach> (unselect BSO, BSF, BSR, EDU and MED, unselect years 2005-2007, then hit "go").

<sup>14</sup> Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007 (M-07-16).

data breach laws which mandate disclosure whenever data is lost, the OMB guidance describes an elaborate risk based trigger where the agency is required to evaluate a series of factors before determining whether to provide notification. In and of itself this type of discretion is very troubling. By their very nature data breaches are embarrassing events for agencies (or any entity) because they often reveal mistakes or poor security practices. Making notice discretionary will give the agency a strong incentive to come down on the side of not providing notice.

The factors and guidance OMB offers agencies in making this determination only exacerbate this problem. For example, part of the background OMB offers to the agency in deciding whether to disclose a breach is:

**“Chilling Effects of Notices.** A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public. In addition, agencies should consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.<sup>15</sup>

It is hard to see how this guidance comports with the fundamental Privacy Act principle of transparency and accurate description of disclosures of records. In fact, it seems like an active invitation to defer notice.

The key criteria OMB offers for determining whether to provide notice are equally problematic. As an initial matter, OMB frames all breach notification requirements in terms of whether the breach is likely to cause harm and the level of risk associated with that harm. While harm is an important criteria, it ignores the other important role that public breach notification plays, namely as an accountability tool that spurs improved security and privacy controls. Small breaches are often indicative of a larger problem in computer security practices, training or other controls. Allowing agencies to paper over those problems is likely to lead to greater problems down the road.

Further, OMB’s evaluation of what might cause harm is flawed. It encourages agencies to consider factors like:

the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.<sup>16</sup>

---

<sup>15</sup> *Id* at 12-13.

<sup>16</sup> *Id* at 15.

These decisions are best made by the individual affected, not the agency. In reality, it is impossible to see how the agency could foresee secondary uses of data. Sometimes even data that most people view as benign, such as name and address, can be very sensitive if associated with a survivor of sexual assault or stalking who has worked very hard to conceal it.

The guidance also authorizes the agency to consider whether the risk can be mitigated by the agency. Naturally the agency should take all mitigation steps but that effort should be completely separate from a decision about whether to notify victims of a breach. Again, all of this guidance is completely contrary to the fundamental purpose of the Privacy Act: to empower citizens with knowledge about and control over how the government handles their personal information.

**Recommendation:** OMB should change its data breach guidance to severely limit the discretion of federal agencies to avoid providing notice to affected parties in the case of a breach. Notice should be triggered whenever personally identifiable data is released in a readable form (not protected by encryption or other security measures).

#### IV. Privacy Act Remedies and Oversight

Since 2008, there have been two significant developments which have served to further erode transparency and accountability under the Privacy Act – the recent Supreme Court case *FAA v. Cooper* and the failure by the President and Congress to fill the Privacy and Civil Liberties Oversight Board (PCLOB).

##### A. *FAA v. Cooper*

In *FAA v. Cooper*, the Supreme Court held that the victims of Privacy Act violations cannot recover damages for mental or emotional distress, no matter how severe, unless they suffer financial harm as a result of the violation.<sup>17</sup> In *Cooper*, the plaintiff’s HIV status was shared by the Social Security Administration with the Federal Aviation Administration (FAA) and Department of Transportation.

In *Cooper*, despite the fact that the agencies violated the Privacy Act, it was unclear whether the plaintiff could recover the damages authorized by 5 U.S.C. 552(a)(g)(4)(A). This section provides that any agency who willfully fails to comply with the Privacy Act is liable for “actual damages sustained by the individual as a result of the... failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000.” At issue was the definition of “actual damages.” In previous decisions, circuits had split over whether “actual damages” meant “general damages,” which allow recovery for emotional harm, or “special damages,” which required pecuniary harms.<sup>18</sup> This definition was important because the plaintiff did not allege an

---

<sup>17</sup> *F.A.A. v. Cooper*, 132 S. Ct. 1441 (2012).

<sup>18</sup> See *Fitzpatrick v. IRS*, 665 F.2d 327, 329-31 (11th Cir.1982) (holding that “actual damages” are limited to proven pecuniary losses); *Johnson v. IRS*, 700 F.2d971, 972 (5th Cir. 1983) (holding that “actual damages” may be

economic loss as a result of the Privacy Act violation. He only claimed to have suffered “humiliation, embarrassment, mental anguish, fear of social ostracism and other severe emotional distress.”<sup>19</sup> The Court concluded that Congress intended through use of the term “actual damages” to mean special damages and limited the availability of recovery under the Privacy Act to those suffering from economic harm. The plaintiff was denied damages for his emotional harm.

This decision has a negative impact on the general privacy protections provided by the Act, as well as on an individual’s ability to recover for harms. The Privacy Act was created in order to provide “a series of basic safeguards... to help remedy the misuse of personal information by the Federal Government and reassert the fundamental rights of personal privacy of all Americans.”<sup>20</sup> Congress viewed the civil damages remedy as key to enforcing the Act and as commentators have noted the deterrent effect presented by the threat of litigation is a significant one.<sup>21</sup> By foreclosing relief for these types of harms, the court weakens protections for precisely the type of harmful disclosure of embarrassing or detrimental information, such as HIV status, that should be a core focus of the Act.

The decision also strips from victims of real harms the ability to recover their damages. The court’s holding is clear. No matter how much emotional pain, humiliation or real mental distress a victim endures, if it is not a pecuniary harm, recovery is barred. In practice the result of this interpretation is that release of much of the information covered by the Privacy Act will fall outside the statutory remedy. For example, recently it was alleged that the 2010 campaign of Washington, D.C. Mayor Vincent Grey improperly used lists of residents of public housing as part of its get out the vote efforts.<sup>22</sup> These lists would be covered by the Privacy Act and contain names, addresses and phone numbers including cell phones. If public housing residents were harmed by this disclosure, for example by receiving harassing phone calls, under *Cooper* they would have no remedy absent a showing of financial harm.

**Recommendation:** The language of the Privacy Act should be modified in 5 U.S.C. 552a(g)(4)(A) to make clear that actual damages extend beyond pecuniary harms and include mental and emotional distress.

## **B. Privacy and Civil Liberties Oversight Board**

---

established by evidence of either financial or non-financial injuries); *Hudson v. Reno*, 130 F.3d 1193, 1206-07 (6th Cir. 1997) (holding that “actual damages” can be established only by evidence pecuniary losses).

<sup>19</sup> *Cooper* at 1447.

<sup>20</sup> *House Comm. on Gov't Operations and Senate Comm. on Gov't Operations*, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 -- S. 3418 (Pub. L. No. 93-579) Source Book on Privacy, 304 (1976) available at [http://www.loc.gov/rr/frd/Military\\_Law/pdf/LH\\_privacy\\_act-1974.pdf](http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf).

<sup>21</sup> Frederick Z. Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611, 622 (1984).

<sup>22</sup> Nikita Stewart and Mike DeBonis, *Mayor Gray's 2010 campaign had database of public-housing residents*, Washington Post, July 22, 2012.

At the recommendation of the 9/11 Commission, in 2004, Congress created the Privacy and Civil Liberties Oversight Board (PCLOB) and later reconstituted it as an independent body in 2007.<sup>23</sup> The PCLOB is tasked with overseeing “the information sharing practices of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to determine whether they appropriately protect privacy and civil liberties”.<sup>24</sup> As such, it has significant oversight authority regarding the type of collection and sharing of personal information regulated by the Privacy Act and could serve as an important check on abuses of the Act.

Unfortunately, President Bush refused to nominate one of the candidates put forth by leaders in Congress who traditionally select the commissioners from the opposite party from the president. In retaliation, the Senate refused to confirm any of Bush’s GOP nominees. Because the terms of the original board members expired in January 2008, the revised board was never brought into existence during President Bush’s term.<sup>25</sup>

Compliance has been no better under President Obama. Despite letters from lawmakers and advocacy groups, he failed to nominate a full slate of candidates for the Board for almost three years. It wasn’t until December 2011 that nominations were sent to the Senate for its consideration.<sup>26</sup> Candidates for the PCLOB have been awaiting action by the full Senate since May.

Given that the board has never existed in its current form it is hard to concretely evaluate the impact it would have on Privacy Act enforcement, however it was a key recommendation of the 9/11 Commission. As the former Chairman Tom Kean and Vice Chairman Lee Hamilton testified before this committee:

If we were issuing grades, the implementation of this recommendation would receive a failing mark. We urge the Administration and Congress to address this failure in a speedy fashion. An array of security-related policies and programs present significant privacy and liberty concerns. A robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind.

---

<sup>23</sup> U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 395. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-408 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801 (2007).

<sup>24</sup> The 9/11 Commission Act of 2007 §801 (d)(2)(B).

<sup>25</sup> Michael Isikoff and Mark Hosenball, “Who’s Watching the Spies?” *Newsweek*, July 9, 2008; online at <http://www.newsweek.com/id/145140>.

<sup>26</sup> The White House, Office of the Press Secretary, *President Obama Announces More Key Administration Posts*, December 15, 2011.



Board review can also give national security officials an extra degree of assurance that their efforts will not be perceived later as violating civil liberties.<sup>27</sup>

While it is unknown how much oversight the PCLOB will eventually exert, it is incontrovertible that it will be impossible for the Board to provide any oversight until members are nominated and confirmed.

**Recommendation:** Nominate and confirm a full slate of board members for the PCLOB and fully staff this vital independent board.

V. Increased use of non-terrorism related information by the National Counterterrorism Center

The steady erosion of privacy protections for personal information held by the federal government has led to an environment where information on Americans can be shared widely for a host of purposes unrelated to the original reason it was collected. Perhaps the most troubling recent example of this trend is the sweeping changes the National Counterterrorism Center (NCTC) made to its guidelines governing how it collects and uses information about US persons not suspected of wrongdoing for intelligence analysis.<sup>28</sup> The new rules effectively remove traditional protections for US person information and allow the vast power of the US Intelligence Community to be turned on innocent Americans. They clearly demonstrate the need to update the Privacy Act and ensure that Americans have real protections for how the information collected by an array of federal government agencies is shared and used.

**A. Changes to the NCTC Guidelines**

Under the new guidelines approved by the Attorney General, NCTC may engage in a variety of troubling new practices including collecting entire databases from federal agencies which mainly consist of information about Americans with no connection to terrorism, and analyzing those databases and disseminating the results for reasons which are also unconnected to terrorism.

The new guidelines accomplish this in a variety of ways. In what is perhaps the most significant change, the Obama administration has extended the authority of the NCTC to intentionally collect, retain and assess data on U.S. citizens and residents, even where those people have no suspected ties to terrorism. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or related to an actual investigation. Therefore, when NCTC collected information from federal

---

<sup>27</sup> *Ten Years After 9/11: A Report From the 9/11 Commission Chairmen, before the Senate Committee on Homeland Security and Governmental Affairs, 112<sup>th</sup> Congress, (2011)* (Testimony Governor Tom Kean and Congressman Lee Hamilton).

<sup>28</sup> National Counterterrorism Center, GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, Released March 22, 2012.

government databases, it had to search for and identify any innocent US person information inadvertently collected, and discard it within 180 days. This crucial purpose limitation meant that NCTC was dissuaded from collecting or maintaining information on innocent Americans in its large databases, and prohibited from using or disseminating it. The 2012 guidelines eliminate this check, allowing NCTC to collect and “continually assess” information on innocent Americans for up to five years.<sup>29</sup>

The new guidelines also effectively broaden an authority previously claimed by NCTC, namely the ability to ingest entire databases maintained by other government agencies. According to the new guidelines, as long as the Director of the NCTC determines that a dataset contains “significant terrorism information,” which is not defined, the NCTC may “acquire and replicate portions or the entirety of a dataset”. While NCTC previously claimed such authority, the retention limits on collection for US persons meant that only datasets consisting almost entirely of terrorism information and/or non-US person information could reasonably be collected using this methodology. The NCTC was dissuaded from swallowing up entire databases consisting of large amounts of innocent US person information by the resource burden of locating and purging it within 180 days. By allowing collection and retention of non-terrorism related US person information for 5 years, the NCTC Guidelines have authorized the NCTC to ingest many new federal databases that consist primarily of non-terrorism related US person information.<sup>30</sup>

Once NCTC acquires this information, the new guidelines give it broad new powers to search through it. As long as queries are designed to solely identify information that is reasonably believed to constitute terrorism information, it may conduct queries that involve non-terrorism data points and pattern based searches and analysis (data mining).<sup>31</sup> It is particularly noteworthy that NCTC relies on a technique, data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be caught up in terrorism investigations if this technique is utilized. As far back as 2008 the National Academy of Sciences found that data mining for terrorism was scientifically “not feasible” as a methodology, and likely to have significant negative impacts on privacy and civil liberties.<sup>32</sup>

Equally disturbing is that once information is gathered and assessed with these tools it can be shared very broadly, in some cases with literally anyone. Such sharing does not have to

---

<sup>29</sup> 2012 Guidelines at 9.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.* at 10.

<sup>32</sup> See National Academy of Sciences report, "Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment" [http://books.nap.edu/catalog.php?record\\_id=12452#toc](http://books.nap.edu/catalog.php?record_id=12452#toc)

be connected to a terrorism investigation. This chart lists some of the types of information NCTC may share, as well as all the entities that can receive this information.<sup>33</sup>

<b>Types of information that can be shared</b>	<b>Individuals and groups that can receive information</b>
Foreign aspects of international narcotics activities	Federal, state, local, tribal, or foreign or international agency that is reasonably believed to need such information
Reasonably appears to be evidence of a crime	Federal, state, local, tribal, or foreign agency which has jurisdiction and that is reasonably believed to need such information
Reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations or (ii) protect against or prevent a crime or a threat to the national security	Federal, state, local, tribal, or foreign entity, or to an individual or entity not part of a government
For the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts	Federal, state, local, tribal, or foreign or international entity
For the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure	Federal, state, local, tribal, or foreign or international entity
Otherwise required by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements	2012 Guidelines are silent on who the sharing would be to, but presumably that would be covered by the statutes, treaties, orders, directives, policies, MOUs or agreements
For the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it	Appropriate elements of the Intelligence Community
Bulk dissemination in support of a legally authorized counterterrorism mission	Other elements of the Intelligence Community

In short, information can be shared for an almost unlimited number of purposes and to a completely unlimited number of individuals. Particularly striking is the authority to share information with anyone (“federal, state, local, tribal, or foreign entity, or to an individual or

<sup>33</sup> *Id* at 13-14.

entity not part of a government”) in order to protect the safety or security of person, property or organizations; or protect against or prevent a crime or a threat to the national security. Such authority seems to provide few limits and almost no guidance to NCTC and other intelligence agencies.

All of this is happening with very little oversight. Controls over the NCTC are mostly internal to the DNI’s office and important oversight bodies such as Congress and the President’s Intelligence Oversight Board aren’t notified of even “significant” failures to comply with the Guidelines.<sup>34</sup> One entity might be able to perform some useful oversight because it does have fairly straightforward authority to “access all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other materials that it deems relevant to its oversight of NCTC activities.” Unfortunately that entity is the PCLOB, which, as described above, has not been seated.

## **B. Privacy Act Impact**

When these practices are viewed through the lens of the supposed protections of the Privacy Act, it is clear how badly the Act is in need of an update. One of the major protections of the Privacy Act is that it bars the sharing of records between agencies except pursuant to specifically delineated exceptions described in subsection (b). None of these exceptions are broad enough to cover this type of wholesale disclosure to the NCTC, nor is there a general national security exception to the Privacy Act. Presumably then, entire databases are being disclosed pursuant to the long abused “routine use” exception described in section II. However, it is difficult to imagine that any American believes that any transaction with the federal government can open them up for screening as a terrorist as long as an agency declares use of that information for that purpose to be “routine”.

Courts have also held that agencies shouldn’t share information with other agencies unless it has compatibility with the purpose for which the information was collected. The modern definition of “compatibility” was established in *Britt v. Naval Investigative Services*, in which the 3<sup>rd</sup> Circuit held there must be “some meaningful degree of convergence between the agencies’ purpose in collecting the information and its disclosure.”<sup>35</sup> The court also noted that the purpose for collection and disclosure should be determined on a case-specific basis. Similarly, in *Swenson v. U.S. Postal Service*, the 9<sup>th</sup> Circuit echoed *Britt’s* holding, and found that there must be a “meaningful degree of convergence” between the purpose for which the information was collected and the reason it was disseminated.<sup>36</sup>

---

<sup>34</sup> *Id* at 17.

<sup>35</sup> 886 F.2d 544 (3<sup>rd</sup> Cir. 1989)

<sup>36</sup> 890 F.2d 1075 (1989)

The NCTC also asserts a series of other exceptions to the Privacy Act. These types of exemptions are authorized under subparts (j) and (k) of the Act and have become commonplace. But a quick review of the exemptions NCTC asserts demonstrates how much control they take away from the subject of the information. NCTC exempts itself from the following requirements for all its databases:

- Subsection (c)(3) (accounting for disclosures),
- Subsections (d)(1)-(4) (record subject's right to access and amend records),
- Subsection (e)(1) (maintain only relevant and necessary records),
- Subsection (e)(4)(G) and (H) (publication of procedures for notifying subjects of the existence of records about them and how they may access records and contest contents),
- Subsection (e)(4)(I) (identifying sources of records in the system of records), and
- subsection (f) (agency rules for notifying subjects to the existence of records about them, for accessing and amending records, and for assessing fees).<sup>37</sup>

In short, NCTC will not guarantee it is using accurate information, account for how it discloses that information, assure that it is relevant or ever let individuals know they have been the subject of an investigation. For obvious reasons the accuracy of the information is of particular concern. Evidence from other database where the collecting agency does not attest to the accuracy of the information indicates that this tends to result in substantial errors.<sup>38</sup>

The federal government collects an enormous amount of personal information. It is necessary in order for citizens to receive benefits and services, to exercise fundamental rights like voting or petitioning the government, for licensing everything from guns to businesses, for employment, education and for many types of health care. In short this information collection is nearly ubiquitous to American life. However under the new NCTC guidelines and the outdated protections of the Privacy Act, providing this information to any federal agency is akin to entering a lineup as a potential terrorist. Nor does the government's sharing this information have to be connected to terrorism at all. Information can be used for national security and safety, drug investigations, if it is evidence of a crime, or simply to evaluate sources or contacts. This boundless sharing is broad enough to encompass disclosures to an employer or landlord about someone who NCTC may think is potentially a criminal, or at the request of local law enforcement for vetting you as a potential informant.

Ultimately, this boundless disclosure, limitless sharing and expansive exemptions seem to create a system of records that is outside the Privacy Act. The only protection offered by the Privacy Act in regard to NCTC is strictly bureaucratic – the agency must declare that a system of records exists and, either explicitly state that many of the provisions of the Privacy Act do not

---

<sup>37</sup> 32 CFR 1701.21

<sup>38</sup> See for example errors in the National Crime Information Center (NCIC) which is collected by the FBI: <http://bjs.ojp.usdoj.gov/content/pub/pdf/umchri01.pdf> and [http://epic.org/privacy/hiibel/epic\\_amicus.pdf](http://epic.org/privacy/hiibel/epic_amicus.pdf)

apply or implicitly exploit loopholes to avoid its requirements. Contrast this with the Congressional finding in support of the Privacy Act:

The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information; ... In order to protect the privacy of individuals identified in information system maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

It is difficult to see how the NCTC's guidelines for handling Americans' personal information meet any of these goals. Unfortunately, this type of broad information sharing is not an isolated occurrence. Instead, broadening definitions of routine use, constant employment of exemptions, use of commercial databases and boilerplate notifications result in a systematic weakening of the Privacy Act and widespread harm to Americans privacy.

**Recommendation:** Congress should prohibit the intelligence community's intentional collection of non-terrorism related US person information. If such information is inadvertently collected it should be immediately identified and removed.

## VI. Conclusion

The Privacy Act and other associated federal data use practices require an overhaul. Their outdated protections are widely circumvented by agencies and the result is the creation of new databases, such as those compiled by the NCTC that violate the spirit of the Privacy Act and harm Americans' privacy.

## **EXHIBIT P**



# New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance

**September 27, 2012**

Justice Department [documents](#) released today by the ACLU reveal that federal law enforcement agencies are increasingly monitoring Americans' electronic communications, and doing so without warrants, sufficient oversight, or meaningful accountability.

The documents, handed over by the government only after months of [litigation](#), are the attorney general's 2010 and 2011 reports on the use of "pen register" and "trap and trace" surveillance powers. The reports show a dramatic increase in the use of these surveillance tools, which are used to gather information about telephone, email, and other Internet communications. The revelations underscore the importance of regulating and overseeing the government's surveillance power. (Our original [Freedom of Information Act request](#) and our legal [complaint](#) are online.)

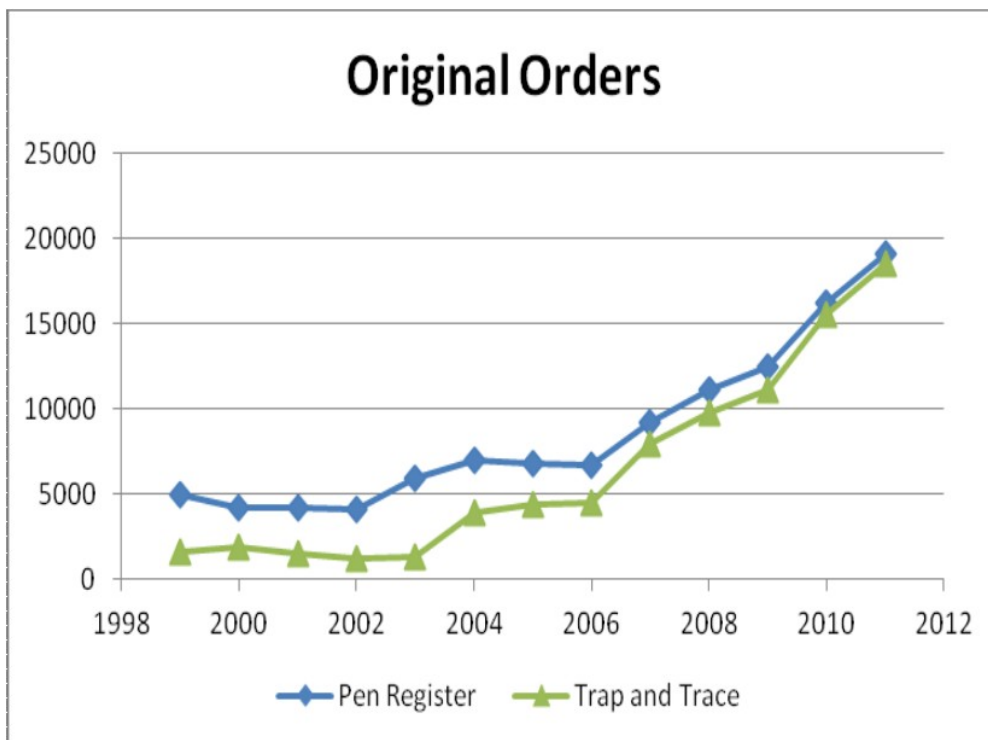
Pen register and trap and trace devices are powerfully invasive [surveillance tools](#) that were, [twenty years ago](#), physical devices that attached to telephone lines in order to covertly record the incoming and outgoing numbers dialed. Today, no special equipment is required to record this information, as interception capabilities are built into phone companies' call-routing hardware.

Pen register and trap and trace devices now generally refer to the surveillance of information *about*—rather than the contents of—communications. Pen registers capture outgoing data, while trap and trace devices capture incoming data. This still includes the phone numbers of incoming and outgoing telephone calls and the time, date, and length of those calls. But the government now also uses this authority to intercept the "to" and "from" addresses of email messages, records about instant message conversations, non-content data associated with social networking identities, and at least some information about the websites that you visit (it isn't entirely clear where the government draws the line between the content of a communication and information about a communication when it comes to the addresses of websites).

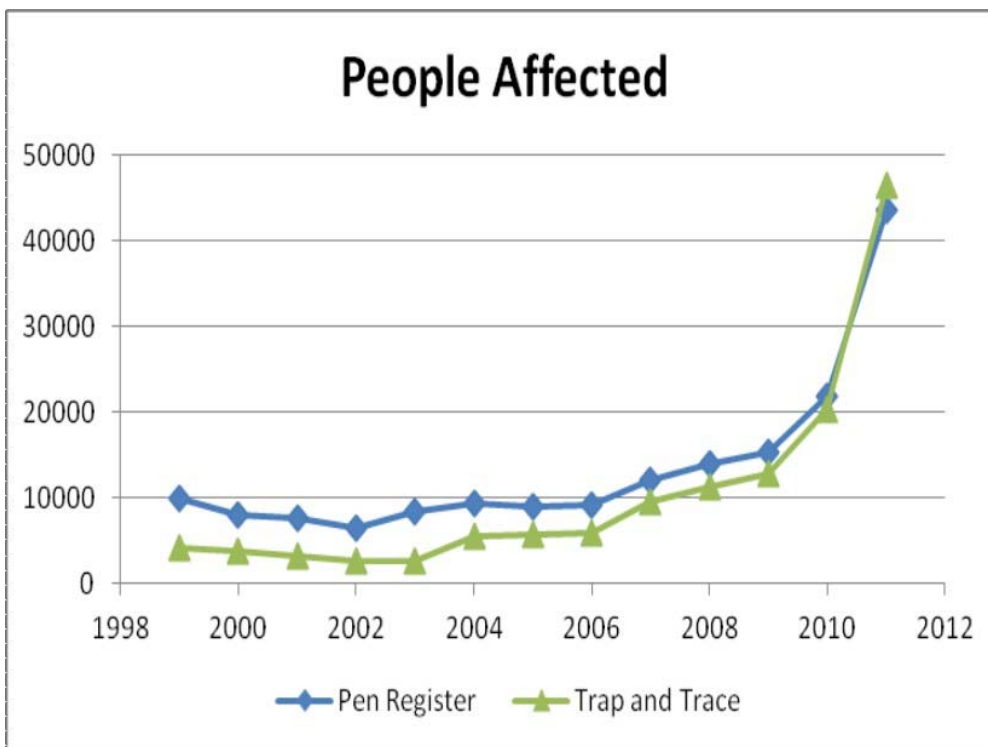
## **Electronic Surveillance Is Sharply on the Rise**

The reports that we received document an enormous increase in the Justice Department's use of pen register and trap and trace surveillance. As the chart below shows, between 2009 and 2011 the combined number of original orders for pen registers and trap and trace devices used to spy on phones increased by 60%, from 23,535 in 2009 to 37,616 in 2011.

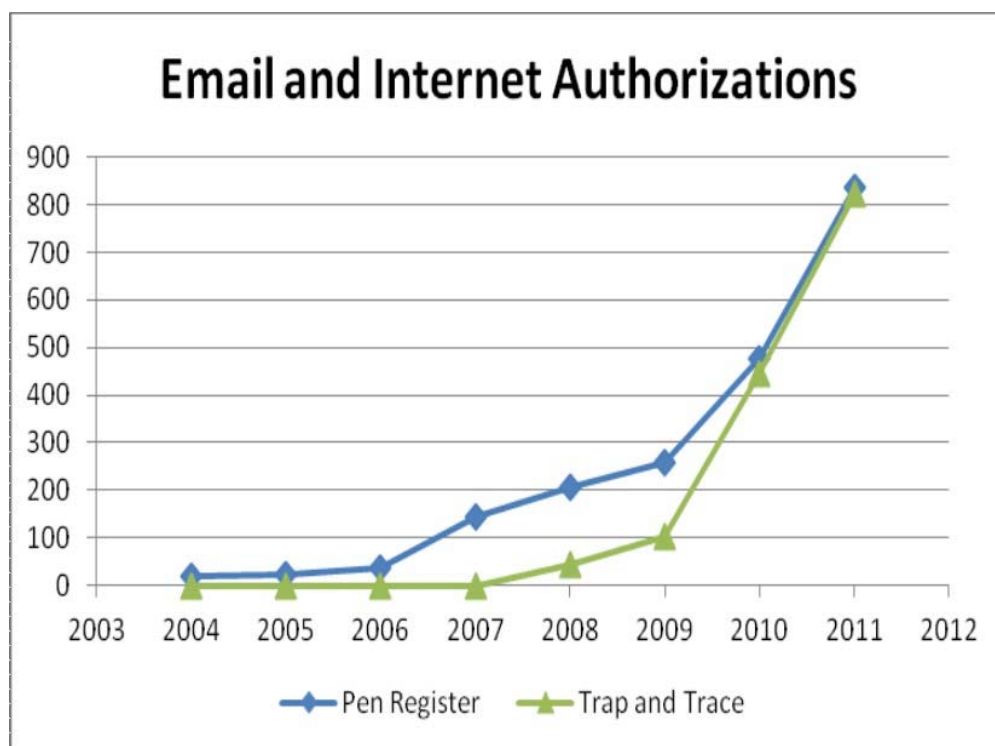




During that same time period, the number of people whose telephones were the subject of pen register and trap and trace surveillance more than tripled. **In fact, more people were subjected to pen register and trap and trace surveillance in the past two years than in the entire previous decade.**



During the past two years, there has also been an increase in the number of pen register and trap and trace orders targeting email and network communications data. While this type of Internet surveillance tool remains relatively rare, its use is increasing exponentially. The number of authorizations the Justice Department received to use these devices on individuals' email and network data increased 361% between 2009 and 2011.



The sharp increase in the use of pen register and trap and trace orders is the latest example of the skyrocketing spying on Americans' electronic communications. Earlier this year, the *New York Times* [reported](#) that cellphone carriers received 1.3 million demands for subscriber information in 2011 alone. And an ACLU public records project [revealed](#) that police departments around the country large and small engage in cell phone location tracking.

#### **Legal Standards For Pen Register And Trap And Trace Orders Are Too Low**

Because these surveillance powers are not used to capture telephone conversations or the bodies of emails, they are classified as “non-content” surveillance tools, as opposed to tools that collect “content,” like wiretaps. This means that the legal standard that law enforcement agencies must meet before using pen registers is [lower](#) than it is for wiretaps and other content-collecting technology. Specifically, in order to wiretap an American's phone, the government must convince a judge that it has sufficient probable cause and that the wiretap is essential to an investigation. But for a pen register, the government need only submit certification to a court stating that it seeks information relevant to an ongoing criminal investigation. As long as it completes this simple procedural requirement, the government may proceed with pen register or trap and trace surveillance, without any judge considering the merits of the request. As one court [noted](#), the judicial role is purely “ministerial in nature.”

The content/non-content distinction from which these starkly different legal requirements arise is based on an erroneous factual premise, specifically that individuals lack a privacy interest in non-content information. This premise is false. Non-content information can still be extremely invasive, revealing who you communicate with in real time and painting a vivid picture of the private details of your life. If reviewing your social networking contacts is sufficient to [determine your sexuality](#), as found in an MIT study a few years ago, think what law enforcement agents could learn about you by having real-time access to whom you email, text, and call. But the low legal standard currently applied to pen register and trap and trace devices allows the government to use these powerful surveillance tools with very little oversight in place to safeguard Americans' privacy.

#### **Failure to Share These Reports with the Public Frustrates Democratic Oversight**

In order to maintain a basic measure of accountability, Congress [requires](#) that the attorney general submit annual reports to Congress on the Justice Department's use of these devices, documenting:

- The period of interceptions authorized by each order and the number and duration of any extensions of each order
- The specific offenses for which each order was granted

- The total number of investigations that involved orders
- The total number of facilities (like phones) affected
- The district applying for and the person authorizing each order.

As my colleague Chris Soghoian has [noted](#), however, the Justice Department has routinely failed to submit the required reports. In fact, the Justice Department repeatedly failed to submit annual reports to Congress between 2000 and 2008 (submitting them instead as “document dumps” covering four years’ worth of surveillance in 2005 and 2009). The department’s repeated failure to follow the law led the Electronic Privacy Information Center to write a [letter of complaint](#) to Senator Patrick Leahy (D-Vt.) in 2009.

Unfortunately, even when the Justice Department does turn over the reports, they have disappeared “into a congressional void,” as Professor Paul Schwartz has put it, instead of being released to the public. The reports for 1999-2003 were [obtained by the Electronic Frontier Foundation](#) through a FOIA request. Chris Soghoian obtained the 2004-2009 reports through the same process.

When no reports surfaced in 2010 and 2011, the ACLU filed a [FOIA request](#) to obtain them. After our request received no response, we [filed suit](#) to enforce it.

Although the Justice Department has in the past repeatedly failed to submit the annual reports to Congress, it appears that it has now cleaned up its act. Both the 2010 and 2011 reports were submitted to Congress in compliance with the reporting requirement. Unfortunately, Congress has done nothing at all to inform the public about the federal government’s use of these invasive surveillance powers. Rather than publishing the reports online, they appear to have filed them away in an office somewhere on Capitol Hill.

This is unacceptable. Congress introduced the pen register reporting requirement in order to impose some transparency on the government’s use of a powerful surveillance tool. For democracy to function, citizens must have access to information that they need to make informed decisions—information such as how and to what extent the government is spying on their private communications. Our representatives in Congress know this, and created the reporting requirement exactly for this reason.

It shouldn’t take a FOIA lawsuit by the ACLU to force the disclosure of these valuable reports. There is nothing stopping Congress from releasing these reports, and doing so routinely. They could easily be posted online, as the ACLU has done today.

Even though we now have the reports, much remains unknown about how the government is using these surveillance tools. Because the existing reporting requirements apply only to surveillance performed by the Department of Justice, we have no idea of how or to what extent these surveillance powers are being used by other law enforcement agencies, such as the Secret Service, Immigration and Customs Enforcement, or state and local police. As a result, the reports likely reveal only a small portion of the use of this surveillance power.

### **Congress Should Pass a Law Improving the Reporting Requirements**

One member of Congress is attempting to overhaul our deeply flawed electronic surveillance laws. In August, Congressman Jerrold Nadler (D-N.Y.) [introduced a bill](#) to amend the [Electronic Communications Privacy Act of 1986](#) to reflect advances in technology that have taken place since the law was passed over twenty-five years ago. One portion of Rep. Nadler’s bill addresses all of the major problems with the current reporting requirements for pen register and trap and trace surveillance. His bill would expand the reporting requirement to apply to all federal agencies, as well as state and local law enforcement. The bill would also shift the responsibility of compiling the reports from the attorney general to the Administrative Office of the United States Courts, which already completes the reporting requirements for the government’s use of wiretaps, and proactively posts those reports on its website each year.

Congressman Nadler’s bill is an opportunity to apply meaningful oversight to the government’s rapidly increasing use of a highly invasive surveillance power. These reforms are critical to protect our privacy and maintain an open and transparent government.

---

Published on *American Civil Liberties Union* (<http://www.aclu.org>)

**Source URL:** <http://www.aclu.org/blog/national-security-technology-and-liberty/new-justice-department-documents-show-huge-increase>

REPORT ON THE USE OF PEN REGISTERS AND  
TRAP AND TRACE DEVICES BY THE LAW ENFORCEMENT AGENCIES/OFFICES  
OF THE DEPARTMENT OF JUSTICE FOR CALENDAR YEAR 2010

<u>PEN REGISTERS</u>	<u>FBI</u>	<u>DEA</u>	<u>USMS</u>	<u>ATF</u>	<u>TOTALS</u>
Original Orders	3,842	4,812	7,266	271	16,191
Extensions	309	960	12	120	1,401
Number of Investigations	1,486	1,231	10,718	106	13,541
Number of Persons Whose Telephone Facilities Were Affected	8,064	5,772	7,278	828	21,942
<u>TRAP AND TRACE DEVICES</u>	<u>FBI</u>	<u>DEA</u>	<u>USMS</u>	<u>ATF</u>	<u>TOTALS</u>
Original Orders	3,285	4,812	7,278	175	15,550
Extensions	266	960	12	77	1,315
Number of Investigations	1,161	1,231	10,718	69	13,179
Number of Persons Whose Telephone Facilities Were Affected	6,832	5,772	7,290	429	20,323
<u>PEN REGISTERS</u>	<u>FBI</u>	<u>DEA</u>	<u>USMS</u>	<u>ATF</u>	<u>TOTALS</u>
Number of Pen Registers Authorized for Email/Networks	115	140	218	5	478
Number of Trap and Trace Devices Authorized for Email/Networks	113	140	191	0	444

## **EXHIBIT Q**

- [Campaign Finance](#)
- [Barack Obama](#)

[More...](#)

# HUFFPOST FUNDRACE data by Aristotle

October 25, 2012

- [FRONT PAGE](#)
- [POLITICS](#)
- [BUSINESS](#)
- [ENTERTAINMENT](#)
- [TECH](#)
- [MEDIA](#)
- [LIFE & STYLE](#)
- [CULTURE](#)
- [COMEDY](#)
- [HEALTHY LIVING](#)
- [WOMEN](#)
- [LOCAL](#)
- [MORE](#)

[POLITICS](#) [POLLSTER](#) [ELECTION 2012](#) [BLOG](#) [2012 ELECTIONS](#) [2012 TOOLBAR](#) [SPECULATRON](#)  
[HUFFPOST HILL](#) [ELECTION DASHBOARD](#) [OFF THE BUS](#) [OCCUPY](#) [CPI](#)

## SEARCH ALL CONTRIBUTORS

Data By Aristotle

City Name

Search Cities

ZIP Code

Search ZIP codes

Last Name  First Name

Search Names

Employer

Search Workplaces

Fundrace makes it easy to search by name or location to see which candidates or political parties your friends, family, co-workers and neighbors are contributing to. Or you can see if your favorite celebrity is putting money where their mouth is and who America's big companies are backing.



**EXHIBIT R**





# Do databases cross a line in border checks?

Posted 4/21/2010 10:32 PM

By Kevin Johnson, USA TODAY



By Dave Einsel for USA TODAY

Former U.S. State Department official Ann Wright has been denied entry to Canada twice because of her misdemeanor arrest record.

[Ann Wright's](#) record of civil disobedience is long and well-documented.

The former [U.S. State Department](#) official, who resigned to protest the [2003 invasion of Iraq](#), doesn't know precisely how many times she's been arrested in public demonstrations against the wars

in [Iraq](#), [Afghanistan](#) and other causes.

But [Canada](#) does.

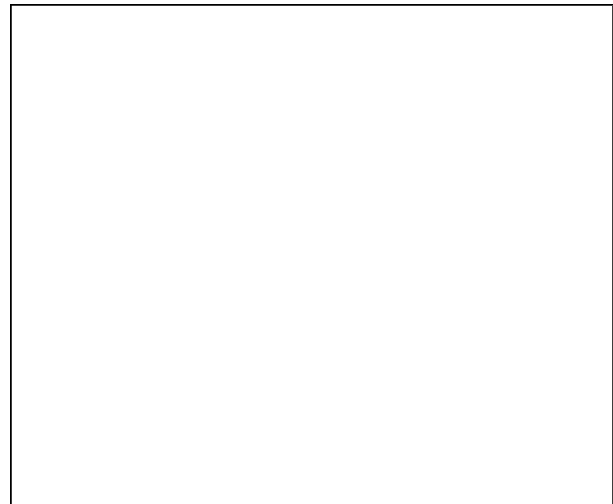
In the past three years, Wright, who lives in [Hawaii](#), has traveled to Canada five times and been denied entry twice. Each of the five times, Canadian authorities questioned the 63-year-old based on their own review of U.S. criminal justice databases containing Wright's misdemeanor arrest record. In 2007, Wright says, she was turned back to the U.S. after being questioned about the prior arrests, despite holding an invitation to [Ottawa](#) from three Canadian Parliament members, who were waiting at the airport to pick her up.

Thousands of times each day, Canadian authorities tap into sensitive U.S. government databases to check the criminal histories of U.S. citizens who are crossing the border or have been entangled in the Canadian criminal justice system, [FBI](#) records show. The databases are an integral part of security operations for Canadian officials, who are preparing for June meetings of the Group of Eight summit of the world's leading economic powers and the G-20 leaders of developed and developing countries. The summit meetings have drawn thousands of protesters in the past, including at last year's G-20 meeting in Pittsburgh.

The databases "provide invaluable investigative assistance" daily for law enforcement and support agencies, the [Royal Canadian Mounted Police \(RCMP\)](#) said in a statement.

During the Winter Olympics, Canadian authorities ran nearly 10,000 criminal history checks per day,

Advertisement



Print Powered By FormatDynamics™



more inquiries than some U.S. states perform each day, FBI records show.

Even more Canadian citizens receive similar scrutiny by U.S. officials with access to Canadian records, according to RCMP records. Since January, Canada has conducted 400,000 queries and the U.S., 1.4 million.

"The whole notion of the sharing of this kind of information in the databases makes people feel very nervous," says MP Libby Davies, one of the members who invited Wright and whose district includes parts of Vancouver. "A case like this does make you question how these databases are being used."

### Keeping close watch

The U.S. shares its criminal databases more freely with Canada than any other country as part of a treaty signed during the [Reagan](#) administration.

FBI officials say the [9/11 terrorist attacks](#) underscored the need for the information exchange, which they believe is key to protecting the homeland.

One of the U.S. government's most important terrorist arrests occurred on the U.S.-Canadian border in 1999, when al-Qaeda operative [Ahmed Ressay](#) tried to smuggle explosives into the U.S. to bomb the Los Angeles International Airport. His 22-year prison sentence was overturned in February by a federal appeals court that called it too lenient.

"Since 9/11, there is a feeling that we have to share this data," which tracks arrest warrants and rosters of missing persons, fugitives and terrorists, said Roy Weise, senior adviser to the FBI's Criminal Justice Information Services Division.

The U.S. has no independent authority to audit Canada's use, Weise says, and Canada has no authority to police U.S. queries of its system. Weise and RCMP Sgt. Greg Cox say the two countries conduct regular internal audits of their own use.

Yet some U.S. and Canadian analysts say the countries' frequent use of the systems raises serious privacy and information security concerns potentially involving millions of people on both sides of the border.

"This is a dangerous practice that needs a tremendous amount of accountability," said Michael German, the [ACLU's](#) national security policy counsel

and a former FBI agent.

He says Canada's access to such detailed — and possibly outdated — personal histories of U.S. citizens, including decades-old misdemeanors, can result in wrongful detention, interrogation and foreign travel bans.

About half of the arrest records in the system have not been updated to reflect convictions, dismissals or acquittals, Weise said, adding that local law enforcement agencies are responsible for giving the FBI updated information.

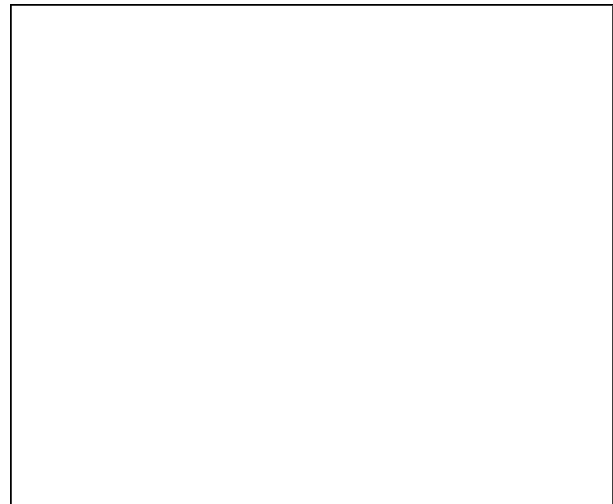
Susan Ginsburg, a former senior staffer on the 9/11 Commission, says privacy and information security laws are "seriously lacking" to keep pace with nations' demands for information to enhance domestic security.

### 'Stunned'

Among the hundreds of people questioned, detained or denied entry during the Winter Olympics were protesters and three California travelers.

One of the California men, Tim Fallman, a 29-year-old Mission Viejo salesman, said he was "stunned" — and a bit embarrassed — when Canadian border authorities grilled him about a trespass violation from 1999. Fallman, wearing only a beanie and goggles, was caught streaking at an Orange County, Calif., high school football game. He and his two companions, who also were questioned about past run-ins with the law, eventually were allowed to enter Canada.

Advertisement

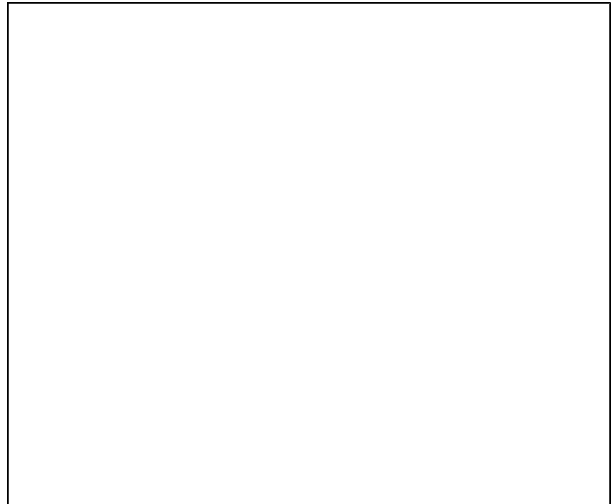


Print Powered By FormatDynamics™



"This is one tool," Cox said of the database. "It is not the sole source of information."

Advertisement



Print Powered By  FormatDynamics™

**The New York Times** Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit [www.nytreprints.com](http://www.nytreprints.com) for samples and additional information. [Order a reprint of this article now.](#)



February 19, 2011

## Can You Frisk a Hard Drive?

By DAVID K. SHIPLER

If you stand with the Customs and Border Protection officers who staff the passport booths at Dulles airport near the nation's capital, their task seems daunting. As a huge crowd of weary travelers shuffle along in serpentine lines, inspectors make quick decisions by asking a few questions (often across language barriers) and watching computer displays that don't go much beyond name, date of birth and codes for a previous customs problem or an outstanding arrest warrant.

The officers are supposed to pick out the possible smugglers, terrorists or child pornographers and send them to secondary screening.

The chosen few — 6.1 million of the 293 million who entered the United States in the year ending Sept. 30, 2010 — get a big letter written on their declaration forms: A for an agriculture check on foodstuffs, B for an immigration issue, and C for a luggage inspection. Into the computer the passport officers type the reasons for the selection, a heads-up to their colleagues in the back room, where more thorough databases are accessible.

And there is where concerns have developed about invasions of privacy, for the most complete records on the travelers may be the ones they are carrying: their laptop computers full of professional and personal e-mail messages, photographs, diaries, legal documents, tax returns, browsing histories and other windows into their lives far beyond anything that could be, or would be, stuffed into a suitcase for a trip abroad. Those revealing digital portraits can be immensely useful to inspectors, who now hunt for criminal activity and security threats by searching and copying people's hard drives, cellphones and other electronic devices, which are sometimes held for weeks of analysis.

Digital inspections raise constitutional questions about how robust the Fourth Amendment's guarantee "against unreasonable searches and seizures" should be on the border, especially in a time of terrorism. A total of 6,671 travelers, 2,995 of them American citizens, had electronic gear searched from Oct. 1, 2008, through June 2, 2010, just a tiny percentage of arrivals.

“But the government’s obligation is to obey the Constitution all the time,” said Catherine Crump, a lawyer for the American Civil Liberties Union. “Moreover, controversial government programs often start small and then grow,” after which “the government argues that it is merely carrying out the same policies it has been carrying out for years.”

One of the regular targets is Pascal Abidor, a Brooklyn-born student getting his Ph.D. in Islamic studies, who reported being frisked, handcuffed, taken off a train from Montreal and locked for several hours in a cell last May, apparently because his computer contained research material in Arabic and news photographs of Hezbollah and Hamas rallies. He said he was questioned about his political and religious views, and his laptop was held for 11 days.

Another is James Yee, a former Muslim chaplain at the Guantánamo Bay prison, who gets what he wryly calls a “V.I.P. escort” whenever he flies into the United States. In 2003, Mr. Yee was jailed and then exonerated by the Army after he had conveyed prisoners’ complaints about abuse, urged respect for their religious practices and reported obscene anti-Muslim caricatures being e-mailed among security staff.

Years later, he evidently remains on a “lookout” list. A federal agent stands at the door of Mr. Yee’s incoming plane, then escorts him to the front of the passport line and to secondary screening.

Arriving in Los Angeles last May from speaking engagements in Malaysia, he was thoroughly questioned and searched, he said, and his laptop was taken for three or four hours. He was not told why, but after it was returned and he was waiting to rebook a connecting flight he’d missed, a customs officer rushed up to the counter. “We left our disk inside your computer,” he quoted her as saying. “I said, ‘It’s mine now.’ She said no, and sure enough when I took the computer out, there was a disk.”

Customs won’t comment on specific cases. “The privacy rights that citizens have really supersede the government’s ability to go into any depth,” said Kelly Ivahnenko, a spokeswoman.

In general, “we’re looking for anyone who might be violating a U.S. law and is posing a threat to the country,” she explained. “We’re in the business of risk mitigation.”

Yet the mitigation itself has created a sense of risk among certain travelers, including lawyers who need to protect attorney-client privilege, business people with proprietary information, researchers who promise their subjects anonymity and photojournalists who may pledge to blur a face to conceal an identity. Some are now taking precautions to minimize data on computers they take overseas.

"I just had to do this myself when I traveled internationally," said Ms. Crump, the lead attorney in a lawsuit challenging the policy on behalf of Mr. Abidor, the National Association of Criminal Defense Lawyers and the National Press Photographers Association.

During a week in Paris, where she lectured on communications privacy, she had legal work to do for clients, which she could not risk the government seeing as she returned. "It's a pain to get a new computer," she said, "wipe it completely clean, travel through the border, put the new data on, wipe it completely clean again."

In simpler days, as customs merely looked for drugs, ivory, undeclared diamonds and other contraband that could be held in an inspector's hand, searches had clear boundaries and unambiguous results.

Either the traveler had banned items, or didn't. Digital information is different. Some is clearly illegal, some only hints at criminal intent, and under existing law, all is vulnerable to the same inspection as hand-carried material on paper.

Most pirated intellectual property and child pornography, for example, cannot be uncovered without fishing around in hard drives. "We've seen a raft of people coming from Southeast Asia with kiddie porn," said Christopher Downing, a supervisor at Dulles. If a person has been gone only two or three days and pictures of children are spotted in a bag, he explained, the laptop is a logical candidate for inspection. Such searches have been fruitful, judging by the bureau's spreadsheets, which list numerous child pornography cases.

But terrorism is an amalgam of violence and ideas, so its potential is harder to define as officers scrutinize words and images as indicators of attitudes, affiliations and aspirations. Random searches are not done, Mr. Downing said, although courts so far have upheld computer inspections without any suspicion of wrongdoing. In practice, something needs to spark an officer's interest. "If you open up a suitcase and see a picture of somebody holding an RPG," he noted, referring to a rocket-propelled grenade, "you'd want to look into that a little more."

The search power is preserved by its judicious use, Mr. Downing said. "If you abuse it, you lose it," he added. The A.C.L.U. doesn't want customs to lose it, Ms. Crump explained, but just wants the courts to require reasonable suspicion, as the Supreme Court did in 1985 for examinations of a person's "alimentary canal." The court distinguished such intrusive inspection from "routine searches" on the border, which "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." The justices added in a footnote that they were not deciding "what level of suspicion, if any, is required for nonroutine border searches" of other kinds.

Laptop searches should be considered “nonroutine,” Ms. Crump argues, something the United States Court of Appeals for the Ninth Circuit declined to do in 2008, when it reversed a judge’s decision to suppress evidence of child pornography obtained during a suspicionless airport computer search.

With the search powers intact, Mr. Abidor no longer dares take the train home from his studies at McGill University in Montreal. He doesn’t want to be stranded at the border, waiting hours for a bus, as he was in May. So on Dec. 22, his father drove up from New York to get him for vacation. The men were ordered to a room and told to keep their hands on a table while customs officers spent 45 minutes searching the car, and possibly the laptop, Mr. Abidor said. “I was told to expect this every time.”

*David K. Shipler, a former reporter at The Times, is the author of “The Rights of the People: How Our Search for Safety Invades Our Liberties,” to be published in April.*

*This article has been revised to reflect the following correction:*

***Correction: March 6, 2011***

*Because of an editing error, an article on Feb. 20 about the inspection of computers at American borders misstated the date that an American, enrolled in Islamic studies in Montreal, returned to the United States by car rather than take a train and risk being stranded at the border while his computer was examined. The crossing took place on Dec. 22, not in January.*

**EXHIBIT S**



**Note:** New York City businesses must comply with all relevant federal, state, and City laws and rules. All laws and rules of the City of New York, including the Consumer Protection Law and Rules, are available through the Public Access Portal, which businesses can access by visiting [www.nyc.gov/consumers](http://www.nyc.gov/consumers). For convenience, sections of the New York City Licensing Law (and Rules, if enacted) are included as a handout in this packet. The Law (and Rules) are current as of January 2009.

Please note that businesses are responsible for knowing and complying with the most current laws, including any City Council amendments. The Department of Consumer Affairs (DCA) is not responsible for errors or omissions in the handout provided in this packet. The information is not legal advice. You can only obtain legal advice from a lawyer.

**NEW YORK CITY ADMINISTRATIVE CODE**  
**TITLE 20: CONSUMER AFFAIRS**  
**CHAPTER 2: LICENSES**  
**SUBCHAPTER 27: GENERAL VENDORS**

§ 20-452 Definitions. For the purposes of this subchapter, the following words and terms shall have the following meaning:

a. "Food". Any raw, cooked, or processed edible substances, beverages, ingredients, ice or water used or intended for use or for sale in whole or in part for human consumption.

b. "General vendor." A person who hawks, peddles, sells, leases or offers to sell or lease, at retail, goods or services, including newspapers, periodicals, books, pamphlets or other similar written matter in a public space. This definition shall not include a food vendor as defined in subdivision c of section 17-306 of chapter three of title seventeen of this code, or a person required to be licensed under section 20-229 of subchapter seven of chapter two of this title of this code. This definition also shall not include persons who use stands or booths in a public space for the shining of shoes. This definition shall not include a pedicab driver licensed in accordance with subchapter nine of this chapter, who is operating a pedicab registered pursuant to subchapter nine and shall not include a pedicab owner licensed pursuant to such subchapter.

c. "General vending business" or "vending business". The business of selling, leasing or offering to sell or lease, at retail, goods or services other than food, engaged in by a general vendor in a public space.

d. "Public space". All publicly owned property between the property lines on a street as such property lines are shown on the City Record including but not limited to a park, plaza, roadway, shoulder, tree space, sidewalk or parking space between such property lines. It shall also include, but not be limited to, publicly owned or leased land, buildings, piers, wharfs, stadiums and terminals.

e. "Pushcart". Any wheeled vehicle or device used by a general vendor

in a public space, other than a motor vehicle or trailer, which may be moved with or without the assistance of a motor and which does not require registration by the department of motor vehicles.

f. "Stand". A movable, portable or collapsible structure, framework, device, container or other contrivance, other than a vehicle or pushcart, used by a general vendor in a public space for the purpose of displaying, keeping or storing any merchandise or article required by him or her while acting as such vendor.

g. "Vehicle". A motor vehicle or trailer, as defined in the vehicle and traffic law.

h. "Vend". To hawk, peddle, sell, lease, offer to sell or lease, at retail, goods or services other than food in a public space.

§ 20-453 License required. It shall be unlawful for any individual to act as a general vendor without having first obtained a license in accordance with the provisions of this subchapter, except that it shall be lawful for a general vendor who hawks, peddles, sells or offers to sell, at retail, only newspapers, periodicals, books, pamphlets or other similar written matter, but no other items required to be licensed by any other provision of this code, to vend such without obtaining a license therefor.

§ 20-454 License term; fees. a. All licenses issued pursuant to this subchapter shall be valid for one year unless sooner suspended or revoked. The commissioner shall establish by regulation the expiration date of such licenses.

b. The commissioner may issue a temporary license upon the furnishing of information and an application in such form and detail as he or she may prescribe and upon the payment of a fee of ten dollars for such temporary license.

c. The annual license fee for a license or a renewal thereof shall be two hundred dollars.

d. The fee for issuing a duplicate license when the original has been lost, destroyed or mutilated shall be ten dollars.

§ 20-455 Applications. a. Each person applying for a general vendor's license or renewal thereof shall file an application in such form and detail as the commissioner may prescribe and, unless exempted by article four of the general business law, shall pay the fee required by this subchapter.

b. In addition to any other information required, the commissioner shall require the following information:

1. The name and home address of the applicant and the name and address

**EXHIBIT T**

# Manual of General Policy

## ARTICLE VI LEGAL

### POLICY 6.1 CONFLICT OF INTEREST

#### **1 General Statement of Policy.**

It is the policy of the University that all of its activities shall be conducted in accordance with the highest standards of integrity and ethics and in a manner that will not reflect or appear to reflect adversely on the University's credibility, objectivity, or fairness. Every individual to whom this Policy is applicable (each, a "Covered Individual") must maintain the highest standards of honesty and integrity and must refrain from any use whatsoever of his or her position at the University, or the information, privileges, or influence such position may provide, when such use is motivated by, or gives the appearance that it is motivated by, the desire for private gain or advantage for the Covered Individual, or for other persons, institutions, or corporations with which he or she has family, professional, business, or financial connections. Accordingly, no Covered Individual shall have any interest, financial or otherwise, direct or indirect, or engage in any business or transaction or professional activity, or incur any obligation of any nature, which is in substantial conflict with the proper discharge of his or her duties and responsibilities at the University.

Sections 2 and 3 of this Policy, which set forth the general standards of conduct and the rules regarding hiring, employment, and contracting decisions and supervisory responsibility involving Family Members, apply to all Covered Individuals. Section 4 sets forth specific obligations of Investigators, whether or not they are Covered Individuals, who are involved in research or similar educational or community outreach activities at the University (collectively, "research") and the University's procedures for reviewing and managing Financial Conflicts of Interest that may arise in connection with such activities. Section 5 sets forth provisions regarding records retention requirements and sanctions for violations of this Policy. Section 6 sets forth the definitions of "Covered Individual", "Family Members", "Financial Conflict of Interest", "Investigator", and other terms used in this Policy. The provisions of this Policy are to be interpreted in light of the paramount importance of academic freedom in the activities of the University.

In the event that Federal, state, or local laws or regulations are enacted (or amended) that require changes in this Policy, the University may amend this Policy, and any related document officially issued by the University to set forth procedures for the implementation of this Policy (each, a "Conflict of Interest Procedural Document"), in order to comply with the new requirements, and such amendment shall not require approval of the University's Board of Trustees.

College and University officials with responsibilities under this Policy are identified by titles that are current as of this Policy's effective date. If the title for a particular position changes at any time, the responsibilities under this Policy shall be performed by the individual having responsibilities within the College or the University similar to the individual who held the former title. If there is a vacancy at any time in the position, the responsibilities under this Policy shall be assumed by the individual to whom such position reports or to his or her designee.

#### **2 General Standards of Conduct.**

Although not all possible situations within the scope of this Policy are included in this Section 2, the following standards, which are primarily based on provisions in New York State Public Officers Law §§ 73 and 74, shall serve as general guidance for Covered Individuals. All Covered Individuals are encouraged to consult the advisory opinions of the New York State Joint Commission on Public Ethics

## **11 Trademarks**

The University owns all right, title and interest in trademarks related to an item of intellectual property owned by the University, or to a program of education, service, public relations, research or training program of the University. ([BTM,2002,11-18,005, B](#))

## **12 Role of the Research Foundation**

The University hereby assigns its ownership rights in inventions resulting from sponsored research to the Research Foundation. The Research Foundation may file patent applications, as named assignee, for such inventions, subject to the terms of this policy, including the distribution provisions set forth in this policy with respect to income earned from the commercialization of such inventions. Furthermore, nothing in this policy shall prevent the Chancellor from appointing the Research Foundation as the Chancellor's designee for performance of the functions assigned to the University in general or to the Chancellor in particular, or to retain distribution of income from commercialization of intellectual property. ([BTM,2002,11-18,005, B](#))

## **13 Effective Date**

This policy is effective from the date of approval by the University Board of Trustees with respect to intellectual property created after that date and shall remain in effect until modified or revoked. ([BTM,2002,11-18,005, B](#))

## **POLICY 6.6 MAINTENANCE OF PUBLIC ORDER**

The Board of Trustees in compliance with Chapter 191 of the Laws of 1969 (Henderson Act) adopts the following rules and regulations for the maintenance of public order on college campuses and other college property used for educational purposes ([BTM,1990,06-25,006, C](#)):

### **1 Rules Governing Members of the Academic Community and Visitors**

A member of the academic community shall not intentionally obstruct and/or forcibly prevent others from the exercise of their rights. Nor shall he or she interfere with the institution's educational processes or facilities, or the rights of those who wish to avail themselves of any of the institution's instructional, personal, administrative, recreational, and community services. ([BTM,1990,06-25,006, C](#))

Individuals are liable for failure to comply with lawful directions issued by representatives of the University/college when they are acting in their official capacities. Members of the academic community are required to show their identification cards when requested to do so by an official of the college. ([BTM,1990,06-25,006, C](#))

Unauthorized occupancy of University/college facilities or blocking access to or from such areas is prohibited. Permission from appropriate college authorities must be obtained for removal, relocation and use of University/college equipment and/or supplies. ([BTM,1990,06-25,006, C](#))

Theft from or damage to University/college premises or property, or theft of or damage to property of any person on University/college premises is prohibited. ([BTM,1990,06-25,006, C](#))

Each member of the academic community or an invited guest has the right to advocate his or her position without having to fear abuse—physical, verbal, or otherwise—from others supporting conflicting points of view. Members of the academic community and other persons on the college grounds shall not use language or take actions reasonably likely to provoke or encourage physical violence by demonstrators, those demonstrated against, or spectators. ([BTM,1990,06-25,006, C](#))

Action may be taken against any and all persons who have no legitimate reason for their presence on any campus within the University/college, or whose presence on any such campus obstructs and/or forcibly prevents others from the exercise of their rights, or whose presence interferes with the

institution's educational processes or facilities, or the rights of those who wish to avail themselves of any of the institution's instructional, personal, administrative, recreational, and community services. ([BTM,1990,06-25,006, C](#))

Disorderly or indecent conduct on University/college-owned or -controlled property is prohibited. ([BTM,1990,06-25,006, C](#))

No individual shall have in his or her possession a rifle, shotgun or firearm or knowingly have in his or her possession any other dangerous instrument or material that can be used and is intended to inflict bodily harm on an individual or damage upon a building or the grounds of the University/college without the written authorization of such educational institution. Nor shall any individual have in his or her possession any other instrument or material that can be used and is intended to inflict bodily harm on any individual or damage upon a building or the grounds of the University/college. ([BTM,1990,06-25,006, C](#))

Any action or situation that recklessly or intentionally endangers mental or physical health or involves the forced consumption of liquor or drugs for the purpose of initiation into or affiliation with any organization is prohibited. ([BTM,1990,06-25,006, C](#))

The unlawful manufacture, distribution, dispensation, possession, or use of illegal drugs or other controlled substances by University students or employees on University/college premises, or as part of any University/college activities is prohibited. Employees of the University must also notify the college personnel director of any criminal drug statute conviction for a violation occurring in the workplace not later than five days after such conviction. ([BTM,1990,06-25,006, C](#))

The unlawful possession, use, or distribution of alcohol by students or employees on University/college premises or as part of any University/college activities is prohibited. ([BTM,1990,06-25,006, C](#))

## **2 Sanctions**

### 2.1 Definitions

- a) Admonition: An oral statement to the offender that he or she has violated university rules
- b) Warning: Notice to the offender, orally or in writing, that continuation or repetition of the wrongful conduct within a period of time stated in the warning, may be cause for more severe disciplinary action
- c) Censure: Written reprimand for violation of a specified regulation, including the possibility of more severe disciplinary sanctions in the event of a conviction for the violation of any University regulation within a period stated in the letter of reprimand
- d) Disciplinary Probation: Exclusion from participation in privileges or extracurricular University activities as set forth in the notice of disciplinary probation for a specified period of time
- e) Restitution: Reimbursement for damage to or misappropriation of property. Reimbursement may take the form of appropriate service to repair or otherwise compensate for damages
- f) Suspension: Exclusion from classes and other privileges or activities, as set forth in the notice of suspension, for a definite period of time
- g) Expulsion: Termination of student status for an indefinite period. The conditions of readmission, if any is permitted, shall be stated in the order of expulsion
- h) Complaint to Civil Authorities
- i) Ejection

Admonition, warning, censure, and disciplinary probation shall be in addition to any other penalty provided by law or The City University. ([BTM,1990,06-25,006, C](#))

## 2.2 Students

Any student engaging in any manner in conduct prohibited under this policy shall be subject to the following range of sanctions defined in this policy ([BTM,1990,06-25,006, C](#)):

- a) Admonition
- b) Warning
- c) Censure
- d) Disciplinary probation
- e) Restitution
- f) Suspension
- g) Expulsion
- h) Ejection
- i) Arrest by the civil authorities

## 2.3 Faculty and Staff

Any tenured or non-tenured faculty member, or other member of the instructional staff, or member of the classified staff engaging in any manner in conduct prohibited under this policy shall be subject to the following range of penalties ([BTM,1990,06-25,006, C](#)):

- a) Warning
- b) Censure
- c) Restitution
- d) Fine not exceeding those permitted by law or by the Bylaws of the University
- e) Suspension with or without pay pending a hearing before an appropriate college authority
- f) Dismissal after a hearing
- g) Ejection
- h) Arrest by the civil authorities

For engaging in the unlawful manufacture, distribution, dispensation, possession, or use of illegal drugs or other controlled substances on University/college premises, or as part of any University/college activities, such an individual may, alternatively, be required to participate satisfactorily in an appropriately licensed drug treatment or rehabilitation program. A tenured or non-tenured faculty member, or other member of the instructional staff, or member of the classified staff charged with engaging in any of these activities shall be entitled to be treated in accordance with applicable provisions of the Education Law or the Civil Service Law, or the applicable collective bargaining agreement, or the Bylaws or written policies of the University. ([BTM,1990,06-25,006, C](#))

## 2.4 Visitors

Any visitor, licensee, or invitee, engaging in any manner in conduct prohibited under this policy shall be subject to ejection, and/or arrest by the civil authorities. ([BTM,1990,06-25,006, C](#))

## 2.5 Organizations

Any organization that authorizes the conduct prohibited under this policy shall have its permission to operate on campus rescinded. ([BTM,1990,06-25,006, C](#))

### **3 Dissemination of Rules and Regulations**

A copy of these rules and regulations is filed with the Regents of the State of New York and with the Commissioner of Education. These rules and regulations are to be incorporated in each college bulletin. ([BTM,1990,06-25,006, C](#))

### **4 Security Services On Campuses**

All security and safety services provided on college-owned or leased facilities shall be the responsibility of the college President. ([BTM,1994,03-21,004, K](#))

College responsibility for security and public safety applies to any building or property owned or controlled by the college and used by the college in direct support of, or related to, its educational purposes, and any building or property owned or controlled by student organizations recognized by the college. This includes student union buildings and other entities that bear the name of the college. ([BTM,1994,03-21,004, K](#))

All security or security related functions at events in college facilities, such as performances, speeches, conferences, meetings, classes, and other special events, shall be managed by the college. No private security personnel, such as bodyguards or escorts acting in a security capacity—with the exception of security guards contracted for by the college—shall perform any campus security or security related functions. The use of armed private security guards is prohibited. ([BTM,1994,03-21,004, K](#))

After consultation with the campus faculty and student constituencies, as well as with the appropriate University offices, the colleges are to establish security and safety guidelines for persons or organizations appearing at campus events or using campus facilities, consistent with this policy. Contracts for speakers or space rentals should contain conditions whereby events may be canceled or payments or deposits may be forfeited for failure to comply with college security policies and procedures. Additionally, any person or organization violating such an agreement may be denied future access to any University campus or related facility in addition to any other applicable college or lawful sanctions. ([BTM,1994,03-21,004, K](#))

This policy does not apply to federal, state, county, or municipal sworn law enforcement officers, or to foreign or international law enforcement personnel who are officially charged with the responsibility of providing security for particular individuals, or who are involved in a law enforcement capacity—e.g. crowd control in conjunction with the security officers of the college. ([BTM,1994,03-21,004, K](#))

This policy, which applies to all facilities and events whether fees are paid to speakers or funded through student fees, is not intended to limit or abridge individual access to or attendance at college events. ([BTM,1994,03-21,004, K](#))

In the event that private security is necessary and requires an exception to this policy, such exceptions must be approved by the college President and the Chancellor and reported to the Board of Trustees' Committee on Fiscal Affairs, Facilities, and Contract Review at the earliest practicable time. ([BTM,1994,03-21,004, K](#))

### **5 Campus Peace Officers**

The Board of Trustees of the University has the power to appoint campus officers who shall have the



powers of peace officers as set forth in the Criminal Procedure Law within the geographical area of the City of New York. The powers of such peace officers include making arrests, searches and issuing appearance tickets, but not the power to carry firearms. It is appropriate to authorize the Chancellor to withhold these powers of peace officers when they are undergoing background checks and training and to suspend them while they are under investigation for misconduct or poor performance, under a disciplinary penalty, and other circumstances. ([BTM,2004,11-29,009, \\_](#))

The Board of Trustees authorizes the Chancellor or his or her designee to withhold and make the initial designation, and to suspend and reinstate the authority and powers as peace officers—under the Criminal Procedure Law of New York State—of campus peace officers who have been appointed by the Board of Trustees. ([BTM,2004,11-29,009, \\_](#))

## **6 Outside Law Enforcement Intervention**

A college president, or his or her designee, shall consult with the Chancellor or his or her designee prior to involving law enforcement agencies during a campus protest, including summoning the police, except in cases of immediate danger to personal safety or to property. In considering such action, the President, or his or her designee, shall make all possible efforts to consult with the student body president(s) and the chair of the faculty governance body. The Chancellor shall endeavor to consult with the student trustee on the President's intent to call the police. ([BTM,1991.01-28,007, A](#))

The Chancellor shall develop a process to be followed by the colleges and the central office prior to calling the police. ([BTM,1991.01-28,007, A](#))

## **7 Violent Felony Offenses and Missing Students**

Each college shall adopt and implement a plan providing for the investigation of any violent felony offense occurring at, or, on the grounds of each such institution, and providing for the investigation of a report of any missing student who resides in a facility owned or operated by the college. Such plans shall provide for the coordination of the investigation of such crimes and reports with the New York City Police Department. (BT1999-11-22,006,\_A)

The Chancellor is authorized to execute such agreements as are necessary with the New York City Police Department providing for the prompt investigation of such violent felony offenses and missing student reports. The plans of each college shall include compliance with the terms of such agreement(s). (BT1999-11-22,006,\_A)

Each college plan must provide for the coordination of the investigation of such reports between the University Public Safety Peace Officer Service and the New York City Police Department in accordance with a written agreement. The University intends to have a master agreement for all of the University colleges with the Police Department. Although the law requires that college plans also include provisions for the reporting and investigation of missing students, this is limited to students residing in dormitories (i.e., facilities owned or operated by the college). (BT1999-11-22,006,\_A)

## **POLICY 6.7 RECORDS RETENTION AND DISPOSITION**

The General Counsel and Vice Chancellor for Legal Affairs, after consultation with the Office of University Management Consulting, shall prepare and distribute uniform Records Retention and Disposition Regulations, specifying minimum retention periods, which are to be followed by all of the colleges and units of the University. ([BTM,1990,02-26,005, B](#))

## **POLICY 6.8 SEXUAL HARASSMENT**

It is the policy of The City University of New York to promote a cooperative work and academic environment in which there exists mutual respect for all University students, faculty, and staff. Harassment of employees or students based upon sex is inconsistent with this objective and contrary to the University's non-discrimination policy. Sexual harassment is illegal under Federal, State, and City laws, and will not be

**EXHIBIT U**

Print

## City of Boston Municipal Code

### 16-12.3 Advertising.

Except in accordance with a permit from the Commissioner of Public Works no person shall, for the purpose of advertising goods, wares or merchandise for sale, while on foot in any street, carry and display any show card, placard or sign, nor shall any person distribute to persons in any street for the purpose of advertising goods, wares or merchandise for sale, handbills, cards, circulars or papers other than newspapers, nor shall any person having the control of any vehicle used principally for advertising permit such vehicle to operate in any street north and east of Massachusetts Avenue. The Commissioner of Public Works shall establish, with respect to such advertising matter, such uniform rules governing the size of show cards, placards, and signs as shall be reasonably necessary to prevent interference with public travel and for the other convenience and safety of the public and such rules governing the size of handbills, cards, circulars and papers other than newspapers which may be distributed in the street as shall be reasonably necessary to prevent littering or other hazard to public safety. Each permit issued hereunder shall contain a copy of the rules relating thereto and shall be limited by its terms to the authorization of conduct permitted thereby and otherwise legal.

No permit shall be required nor shall this ordinance operate to affect, interfere with or in any way abridge the right of persons on the street to carry or display noncommercial show cards, placards or signs or to distribute non-commercial handbills, cards, circulars or papers other than newspapers.

(CBC 1975 Ord. T14 § 287)

**Disclaimer:**

This Code of Ordinances and/or any other documents that appear on this site may not reflect the most current legislation adopted by the Municipality. American Legal Publishing Corporation provides these documents for informational purposes only. These documents should not be relied upon as the definitive authority for local legislation. Additionally, the formatting and pagination of the posted documents varies from the formatting and pagination of the official copy. The official printed copy of a Code of Ordinances should be consulted prior to any action being taken.

For further information regarding the official version of any of this Code of Ordinances or other documents posted on this site, please contact the Municipality directly or contact American Legal Publishing toll-free at 800-445-5588.

© 2011 American Legal Publishing Corporation  
[techsupport@amlegal.com](mailto:techsupport@amlegal.com)  
1.800.445.5588.

**EXHIBIT V**

Print

Berwyn, ILs Code of Ordinances

**§ 860.01 DEFINITIONS.**

For the purpose of this chapter, the following definitions shall apply unless the context clearly indicates or requires a different meaning.

**ICE CREAM PEDDLER.** A peddler who engages, in whole or in part, in the sale or offering for sale of ice cream products.

**ITINERANT VENDOR.** An itinerant merchant or a person who, by himself or herself or by another, in the city, engages in or conducts a temporary or transient business of selling goods, wares or merchandise with the intention of continuing in the business in the city for a period of not more than 120 days, and who, for the purpose of carrying on the business, uses, leases or occupies, either in whole or in part, a room, building or other structure for the exhibition and sale of goods, wares or merchandise. All regulations applicable to peddlers shall apply to **ITINERANT VENDORS**, except § 860.05.

**PEDDLER.** A person who engages in peddling.

**PEDDLING.** The sale or offering for sale of property for immediate delivery from other than a fixed place of business on private property, not including:

(1) The sale of religious books or pamphlets; and

(2) The sale of goods by charitable organizations for charitable purposes on not more than one day in a calendar year.

**SOLICITING or SOLICITATION.** Includes the following:

(1) *Commercial soliciting.* The selling or offering for sale of property, including religious books or pamphlets, for future delivery from other than a fixed place of business on private property;

(2) *Fund soliciting.* Soliciting of funds not involving the sale of property, including solicitation where religious pamphlets or books are given or sold to a donor of funds; and

(3) *Other soliciting.* Other soliciting, including soliciting support for political, charitable or other causes, not involving the solicitation of funds.

(Ord. passed 7-11-1983; Ord. 95-15, passed 4-11-1995)

**§ 860.02 LICENSES.**

(A) *Required.* Every person engaging in the business of peddling, commercial soliciting or itinerant vending must obtain a license therefor from the city, as provided in this section.

(B) *Applications.* An application for the license shall be made upon a form provided by the City Collector. In addition to the information required in a business license application under Chapter 801, the applicant shall truthfully state the following:

- (1) The name of the applicant, the address of his or her present place of residence and length of residence at the address, the business address of the applicant if other than his or her residence address and his or her Social Security number;
- (2) The address of his or her place of residence during the past three years, if other than his or her present address;
- (3) A physical description of the applicant;
- (4) The name and address of the person by whom the applicant is employed or whom he or she represents, and the length of time of employment or representation;
- (5) The name and address of the applicant's employer during the past three years, if other than his or her present employer;
- (6) A description, sufficient for identification, of the subject matter of the soliciting in which the applicant will engage;
- (7) The period of time for which the license is sought;
- (8) The date, or approximate date, of the latest previous application for a license under this chapter, if any;
- (9) Whether a license issued to the applicant by the city or any other municipality has ever been revoked;
- (10) Whether the applicant has ever been convicted of a violation of any of the provisions of this chapter or any other ordinance of the city or any other state municipality regulating soliciting;
- (11) Evidence that the applicant is authorized to solicit for the organization represented; and
- (12) Whether the applicant has been convicted of a felony within the preceding ten years, or convicted of a misdemeanor or ordinance violation within the preceding five years, and the nature of the offense.

(C) *Issuance.* The license application shall be investigated by the Police Department. If the investigation of the application discloses a conviction of a misdemeanor or a felony or the prior revocation of a license, or a conviction of a violation of any ordinance, regulating peddlers or solicitors, if the conviction of a felony has occurred within the last ten years and if the conviction of a misdemeanor, ordinance violation or revocation of a license has occurred within the last five years and if the conviction bears a reasonable relationship to the peddling and soliciting activities intended to be performed by the licensee, then the license shall not be issued. In all other cases, upon payment of the license fee set forth in § 801.13(AAA) and upon compliance with the provisions of these Codified Ordinances relating to business licenses, the license shall be issued within seven days of the application.

(D) *Revocation.* A license issued to a peddler or solicitor under this chapter may be revoked, after proper notice and hearing, because of a violation of any of the provisions of this chapter or any other ordinance of the city or state or federal law, or whenever the licensee ceases to possess the qualifications and character required in this chapter for the original application.

(Ord. passed 7-11-1983)

**Disclaimer:**

This Code of Ordinances and/or any other documents that appear on this site may not reflect the most current legislation adopted by the Municipality.

American Legal Publishing Corporation provides these documents for informational purposes only. These documents should not be relied upon as the definitive authority for local legislation. Additionally, the formatting and pagination of the posted documents varies from the formatting and pagination of the official copy. The official printed copy of a Code of Ordinances should be consulted prior to any action being taken.

For further information regarding the official version of any of this Code of Ordinances or other documents posted on this site, please contact the Municipality directly or contact American Legal Publishing toll-free at 800-445-5588.

© 2011 American Legal Publishing Corporation  
[techsupport@amlegal.com](mailto:techsupport@amlegal.com)  
1.800.445.5588.

**EXHIBIT W**



Laurel, Maryland, Code of Ordinances >> Chapter 8 - LICENSES, PERMITS AND BUSINESS REGULATIONS >>  
ARTICLE V. - VENDING, PEDDLING AND SOLICITING >>

---

## ARTICLE V. - VENDING, PEDDLING AND SOLICITING

---

[Sec. 8-51. - Definitions.](#)

[Sec. 8-52. - License required.](#)

[Sec. 8-53. - Application for license.](#)

[Sec. 8-54. - Issuance of license.](#)

[Sec. 8-55. - Special events.](#)

[Sec. 8-56. - License fees.](#)

[Sec. 8-57. - Display of identification badges and other permits.](#)

[Sec. 8-58. - Notification of name or address change.](#)

[Sec. 8-59. - Exemptions.](#)

[Sec. 8-60. - Claims of exemption.](#)

[Sec. 8-61. - Hours of operation.](#)

[Sec. 8-62. - Littering and trash removal.](#)

[Sec. 8-63. - Vending restrictions.](#)

[Sec. 8-64. - Prohibited conduct.](#)

[Sec. 8-65. - Penalties.](#)

[Sec. 8-66. - Suspension and revocation of license.](#)

[Sec. 8-67. - Appeals.](#)

[Sec. 8-68. - Renewals.](#)

[Sec. 8-69. - Severability.](#)

### Sec. 8-51. - Definitions.

- (a) When used in this chapter, the following words, terms, and phrases, and their derivations, shall have the meanings ascribed to them in this article, except where the context clearly indicates a different meaning:

*City administrator* means the city administrator for the city or their designee.

*Conveyance* includes any public or privately owned vehicle, method or means of transporting people, bicycles, motorized or nonmotorized vehicle, handcart, pushcart, lunch wagon or any other device or thing, whether or not mounted on wheels.

*Department* means the city department of community planning and business services or any of its officials, officers, or employees.

*Goods, wares, merchandise* shall include but not be limited to fruits, vegetables, farm products or provisions, dairy products, fish, game, poultry, meat, plants, flowers, appliances, wearing apparel, jewelry, ornaments, art work, cosmetics and beauty aids, health products, medicines, household needs or furnishings, food of any kind, whether or not for immediate consumption, confections or drinks.

*Motor vehicle* means any vehicle used for displaying, storing, or transporting articles for sale by a vendor and which is required to be licensed and registered by the department of motor vehicles of any state.

*Public space* includes all city-owned parks and city-owned property.

*Public way* means all areas legally open to public use such as public space, public streets, sidewalks, roadways, highways, parkways, alleys, parks, as well as the areas surrounding and immediately adjacent to public buildings.

*Pushcart* means any wheeled vehicle approved by the department of community planning and business services in accordance with this article, designed for carrying property and for being pushed by a person without the assistance of a motor or motor vehicle.

*Sidewalk* means all that area legally open to public use as a pedestrian public way between the curb line and the legal building line of the abutting property.

*Solicitor/peddler*. See "vending."

*Special event* means any occasion including but not limited to fairs, shows, exhibitions, citywide celebrations, and festivals taking place within a specifically defined area of the city for a period of time not to exceed seven (7) days.

*Stand* means any showcase, table, bench, rack, handcart, pushcart, stall or any other fixture or device that is used for the purpose of displaying, exhibiting, carrying, transporting, storing, selling or offering for sale any food, beverages, goods, wares or merchandise upon a sidewalk.

*Street* means all that area legally open to public use as public streets, and sidewalks, roadways, highways, parkways, alleys and any other public way.

*Vending* means any person, traveling by foot, wagon, vehicle or any other type of conveyance from street to street carrying, conveying, or transporting goods, wares or merchandise and offering and exposing them for sale, or making sales and delivering articles to purchasers; or who, without traveling from place to place, exhibits, displays, sells or offers for sale such products from a wagon, handcart, pushcart, motor vehicle, conveyance or from his person while on the public ways of the city. *Vending* also includes any street vendor, hawker, huckster, itinerant merchant, peddler, solicitor or transient vendor. This definition does not include a door-to-door peddler or solicitor which is regulated under article III of this chapter.

*Vehicle* means every device in, upon, or by which a person or property may be transported or drawn upon a street or sidewalk, including, but not limited to, devices moved by human power.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-52. - License required.**

It shall be unlawful for any person to engage in vending unless the person has first obtained a license for the department of budget and personnel services with the concurrence of the director of community planning and business services, upon proper application therefore made in writing and upon payment of the prescribed license fee. All licenses shall be issued according to regulations established by the department of community planning and business services.

(Ord. No. 1660, 11-23-09; Ord. No. 1686, 9-27-10)

### **Sec. 8-53. - Application for license.**

- (a) The application for a vending license shall contain all information relevant and necessary to determine whether a particular license may be issued, including but not limited to:
- (1) The applicant's full name, current address, telephone number and proof of identity, issued by the State of Maryland, or other recognized government;
  - (2) A brief description of the nature, character and quality of goods, wares or merchandise to be offered for sale;

- (3) The specific location, if any, in which the vendor intends to conduct business;
  - (4) If the applicant is employed by another, the name and address of the person, film, association, organization, company or corporation;
  - (5) If a motor vehicle is to be used, a description of the vehicle together with the motor vehicle identification number and license number;
  - (6) A complete listing of any other licenses or permits issued to the applicant by the city within the five (5) years immediately preceding the date of the application.
- (b) *Food and beverage vendors.*
- (1) Unless specifically allowed by the city for a special event, no license for food and/or beverage vendors shall be issued except for pre-packaged, pre-prepared food stuffs, soft serve ice cream/frozen yogurt or shaved ice or other frozen novelties. Food that needs to be prepared on or near the vending vehicle, whether by heating, mixing or any other means of cooking or preparation shall not be licensed or allowed except pursuant to this subsection.
  - (2) Any application for a vending license to engage in the sale of food or beverages shall also be referred to the county and state health department for approval and issuance of a certificate of health inspection (or health permit) in addition to the regular vending license. The applicant's equipment shall be subject to inspections at the time of application and at periodic intervals thereafter. The city will not issue or renew a vending license until all required county or state licenses or permits have been issued and evidence of such, to the reasonable satisfaction of the department, has been demonstrated.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-54. - Issuance of license.**

- (a) The applicant shall be notified in writing by the department of the city's decision to issue or deny the vending license not later than thirty (30) days after the applicant has filed a completed application with the department. The department can add such reasonable conditions or restrictions to the license as reasonably necessary to protect the public safety and the purposes of this article. Any applicant for a license to sell food and beverages as a vendor can only be issued after the applicant receives the approval of the applicable state and/or county departments or agencies.
- (b) Each license shall show the name and address of the licensee, the type of license issued, the kind of goods to be sold, the amount of the license fee, the date of issuance, the license number, an identifying description of any vehicle or conveyance used by the licensee plus, where applicable, the motor vehicle identification number and a copy of any state issued photo identification. Each license shall also show the expiration date of the license and the vendor's permit number which is issued by the city and any conditions or restrictions.
- (c) All licenses, permits and/or identification badges issued under this section are valid for one (1) year unless suspended or revoked and shall be both nonassignable and nontransferable.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-55. - Special events.**

Any vendor wishing to conduct business at a special event shall apply to the department of community planning and business services for a temporary vending permit. Application for such a permit must be made at least five (5) days prior to the beginning of the event for which the permit is sought. The permit shall be valid only for the duration of the special event. Fees for such permit shall be as specified in [section 8-6](#), miscellaneous license fees of this chapter (chapter 8). Any vendor to whom a temporary permit is granted shall be subject to the same operating regulations as all other vendors, except where otherwise specified. Vending at special events without a temporary vending permit is prohibited.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-56. - License fees.**

Any vendor granted a vending license under this article shall pay an annual license fee as set by the mayor. Any vendor granted a temporary vending permit for special events shall pay a fee. The mayor shall set a reasonable fee to be paid for vending license and temporary vending permits for special events and may change such fee periodically as necessary.

*(Ord. No. 1660, 11-23-09; Ord. No. 1686, 9-27-10)*

### **Sec. 8-57. - Display of identification badges and other permits.**

- (a) Any license or permit issued by the department shall be carried with the licensee whenever he/she is engaged in vending. Certificates of health inspection shall also be properly and conspicuously displayed at all times during the operation of the vending business.
- (b) A certificate of health inspection shall be deemed to be properly displayed when attached to the vending pushcart, vehicle, stand or other conveyance, and clearly visible to the public and law enforcement officials.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-58. - Notification of name or address change.**

All vendors shall assure that a current and correct name; residence address and mailing address are on file with the department of community planning and business services. Whenever either the name or address provided by a licensed vendor on his application for a vending license changes, the licensee shall notify the department in writing within fifteen (15) days of such change and provide the same with the name change or address change.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-59. - Exemptions.**

The provisions of this article do not apply to:

- (1) Goods, wares, or merchandise temporarily deposited on the sidewalk in the ordinary course of delivery, shipment or transfer;
- (2) The placing and maintenance of unattended stands or sales devices for the sale, display or offering for sale of newspapers, magazines, periodicals and paperbound books; or
- (3) The distribution of free samples of goods, wares and merchandise by any individual from his person.
- (4) The selling or attempting to obtain orders for the sale of goods, wares, merchandise, services or foodstuffs for any charitable or nonprofit association, organization, corporation or project, provided that the charitable or nonprofit association, organization, corporation or project registers annually with the city administrator.

The charitable or nonprofit association, organization, corporation or project registering under this subsection shall submit each year a form furnished by the city administrator giving, as applicable, its name, address, telephone number, the name of a contact person, a description of its proposed peddling or soliciting activities to the extent known, the location and date of the activities to the extent known, and the number or approximate number of individuals who will engage in the activities.

If during the period a charitable or nonprofit association, organization, corporation or project is registered there is any change in the factual information furnished to the administrator under this subsection, the new information shall be fully and promptly communicated in writing to the city administrator upon a form furnished by the administrator.

- (5) Any person engaged in voter registration activities or partisan or nonpartisan election campaigns, including persons supporting or working against a ballot question.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-60. - Claims of exemption.**

Any person claiming to be legally exempt from the regulations set forth in this article, or from the payment of a license fee, shall cite to the department the statute or other legal authority under which exemption is claimed and shall present to the department proof of qualification for such exemption.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-61. - Hours of operation.**

Unless the license specifically provides otherwise, vendors shall be allowed to engage in the business of vending only between the hours of 9:00 a.m. and 8:00 p.m. each day. No vending station, conveyance or other items related to the operation of a vending business shall be located on any city sidewalk or other public way during nonvending hours.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-62. - Littering and trash removal.**

- (a) Vendors shall keep the sidewalks, roadways and other spaces adjacent to their vending sites or locations clean and free of paper, peelings and refuse of any kind generated from the operation of their businesses. All trash or debris accumulating within twenty-five (25) feet of any vending stand shall be collected by the vendor and deposited in a trash container.
- (b) Persons engaged in food vending shall affix to their vending station, vehicle, pushcart or other conveyance a receptacle for litter that shall be maintained and emptied regularly and marked as being for litter.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-63. - Vending restrictions.**

Absent an explicit authorization by the city for a special event or circumstance, no vendor shall be permitted to operate:

- (1) On any public space, within twenty-five (25) feet of any public right-of-way, street, intersection or pedestrian crosswalk.
- (2) Within twenty-five (25) feet of any, loading zone or bus stop, intersection or pedestrian crosswalk.
- (3) Within two hundred (200) feet of another vending location assigned to another vendor on a public sidewalk.
- (4) In any area within one hundred (100) feet of a building entrance or exit or, in the case of a hotel or motel, within two hundred fifty (250) feet of building entrances or exits.
- (5) Within fifty (50) feet of display windows of fixed location businesses.
- (6) Any area within one thousand (1,000) feet of a hospital, college, university, elementary school, middle school or high school, state or federal building.
- (7) Within twenty-five (25) feet of any fire hydrant or fire escape.
- (8) Within twenty-five (25) feet of any parking space or access ramp designated for persons with disabilities.

(Ord. No. 1660, 11-23-09)

### **Sec. 8-64. - Prohibited conduct.**

No person engaged in the business of vending under this article shall do any of the following:

- (1) Obstruct pedestrian or motor vehicle traffic flow, except for no more than two (2) minutes to load and unload vending stations and/or vending merchandise.
- (2) Obstruct traffic signals or regulatory signs.
- (3) Stop, stand or park any vehicle, pushcart or conveyance upon any street for the purpose of selling during the hours when parking, stopping and standing have been prohibited by signs or curb markings.
- (4) Leave any conveyance unattended at any time or store, park, or leave such conveyance in a public space overnight.
- (5) Use a handcart or pushcart whose dimensions exceed six (6) feet in width, six (6) feet in length, and five (5) feet in height.
- (6) Use any stand or other fixed-location conveyance whose dimensions exceed six (6) feet in width, six (6) feet in length, and three (3) feet in height.
- (7) Use any conveyance that when fully loaded with merchandise, cannot be easily moved and maintained under control by the licensee, his employee, or an attendant.
- (8) Sell any goods, wares or merchandise on public space unless the location has been or shall be hereafter so designated by the mayor and city council for vending.
- (9) Sound any device that produces a loud and raucous noise or operate any loudspeaker, public address system, radio, sound amplifier, or similar device to attract public attention, or otherwise violate [chapter 9](#), article VII, noise control of the Laurel City Code or the Ann. Code of Maryland, Transportation Article § 22-401, horns and warning devices and § 22-401.1, bells on ice cream sales vehicles, as amended.
- (10) Conduct business in such a way as would restrict or interfere with the ingress or egress of the abutting property owner or tenant, create a nuisance, increase traffic congestion or delay, constitute a hazard to traffic, life or property, or obstruct adequate access to emergency and sanitation vehicles.
- (11) Operate in violation of the terms and conditions of the city permit or in violation of the vending restrictions above.
- (12) Operate in violation of the hours and times outlined in section 8-61, hours of operation, above.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-65. - Penalties.**

Violation of this article shall be a municipal infraction. The penalty for violating a provision of this article or any other applicable article of the city code shall be a fine of two hundred fifty dollars (\$250.00) together with revocation or suspension of the vendor's license for a time period not to exceed ninety (90) days for such first offense. Subsequent violations shall be a fine of five hundred dollars (\$500.00) with revocation or suspension of the vendor's license for a time period not to exceed one hundred twenty (120) days. The department of community planning and business services or the police department may enforce this subsection.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-66. - Suspension and revocation of license.**

- (a) In addition to the penalties contained above, any license issued under this article may be suspended or revoked for any of the following reasons:
  - (1) Fraud, misrepresentation or knowingly false statement contained in the application for the

- license;
- (2) Fraud, misrepresentation or knowingly false statement in the course of carrying on the business of vending;
  - (3) Conducting the business of vending in any manner contrary to the conditions of the license or to a direct order by the department or the police;
  - (4) Conducting the business of vending in such a manner as to create a public nuisance, cause a breach of the peace, constitute a danger to the public health, safety, welfare or morals, or interfere with the rights of abutting property owners; or
  - (5) Cancellation or suspension of health department authorization for a food or beverage vending unit due to uncorrected health or sanitation violations or cancellation or suspension of a required county or state license or permit.
- (b) The department shall provide written notice of the suspension or revocation in a brief statement setting forth the complaint, the grounds for suspension or revocation, and notifying the licensee or permittee of his right to appeal. Such notice shall be mailed to the address shown on the license holder's application by certified mail, return receipt requested.
  - (c) If the city revokes a vending license or permit, the fee already paid for the license or permit shall be forfeited. A person whose license or permit has been revoked under this section may not apply for a new license for a period of one (1) year from the date that the revocation took effect.
  - (d) Upon revocation or suspension, the licensee shall immediately return their license to the department of community planning and business services personally or through the police department or other authorized agent; and upon failure to do so, the department may request and direct that the license be confiscated and held pending final disposition.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-67. - Appeals.**

- (a) If the department denies the issuance of a license or permit, suspends or revokes a license or permit, or orders the cessation of any part of the business operation conducted under the license or permit, the aggrieved party may appeal the department's decision to the city administrator.
- (b) Any party aggrieved by a decision of the city administrator with respect to the denial, suspension, or revocation of a license shall have the right to appeal any such decision in writing to the board of appeal for the City of Laurel within thirty (30) calendar days after the date of the denial, suspension or revocation decision rendered by the city administrator, appeals to the board of appeals from denial, suspension or revocation decisions of the city administrator shall be on the record of the hearing before the city administrator.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-68. - Renewals.**

A vending license may be renewed, provided an application for renewal and license fees are received by the city no later than the expiration date of the current license. Any application received after that date shall be processed as a new application. The department shall review each application for renewal, and upon determining that the applicant is in full compliance with the provisions of this article and all applicable city, county and state codes and regulations, shall issue a new license.

*(Ord. No. 1660, 11-23-09)*

### **Sec. 8-69. - Severability.**

The provisions of this article are declared separate and severable. If any clause, sentence, paragraph, subdivision, section, subsection or portion of this article or the application thereof to any person or circumstance is held to be invalid, it shall not affect the validity of the remainder of this article or the

validity of its application to other persons or circumstances.

(Ord. No. 1660, 11-23-09)

### SCHEDULE A. LICENSE FEE SCHEDULE

For the businesses and activities enumerated in this [Chapter 8](#) of the City Code, the following license fees shall be paid; and the fees herein provided are annual, unless otherwise specified:

Business/Activity	Fee
Alcoholic beverages	Twenty (20) percent of the fee charged by the board of license commissioners for Prince George's County
Amusements	\$75.00—Each electronic or mechanical device
Billiard rooms and poolrooms	\$50.00—First table \$25.00—Each additional table
Carnival	\$100.00—Per day
Circus	\$100.00—Per day
<i>Dances</i> , in a public hall	\$100.00—Per dance
Door-to-door solicitation	\$45.00—First year (\$25.00 if applicant provides a criminal background check satisfactory to the city administrator)  \$45.00—Annual renewal (\$25.00 if applicant provides a criminal background check satisfactory to the city administrator)  \$25.00—For replacement of lost or mutilated license
<i>Ice cream or ice cream products sales</i> , from a movable vehicle	\$100.00—Each vehicle operating within the city—Yearly permit required
Live entertainment	\$500.00—Any establishment which provides live entertainment of any kind other than "theatrical exhibitions" for which licensing is required pursuant to <a href="#">section 8-1</a> . License required, of the City Code
<i>Meals, sandwiches, snack foods, beverages or other food items sales</i> , from a movable vehicle	\$100.00—Each vehicle operating within the city—Yearly permit required
Juke boxes and player pianos	\$15.00—Per operating machine
Vending, peddling, and soliciting	\$100.00  \$50.00—Temporary special event  \$25.00—Replacement of lost or mutilated license

(Ord. No. 1686, 9-27-10)

### SCHEDULE B. PERMIT FEE SCHEDULE

For activities enumerated in this [Chapter 8](#) of the City Code, the following permit fees shall be paid; and the fees herein provided are annual, unless otherwise specified:

Permit	Fee
Burglar and holdup alarm user permits	\$50.00—First year (nonrefundable)  \$15.00—Annual renewal



	\$5.00—Duplicate registration sticker
Portable storage container permit	\$25.00—Initial fee
	\$25.00—Per extension

*(Ord. No. 1686, 9-27-10)*

**EXHIBIT X**

Miami, Florida, Code of Ordinances >> PART II - THE CODE >> Chapter 39 - PEDDLERS AND ITINERANT VENDORS >> ARTICLE II. - SIDEWALK AND STREET VENDORS >>

---

## ARTICLE II. - SIDEWALK AND STREET VENDORS

---

[Sec. 39-26. - Definitions.](#)

[Sec. 39-27. - Intent of article.](#)

[Sec. 39-28. - BTR required.](#)

[Sec. 39-29. - License not applicable in certain areas of the city during certain time periods.](#)

[Sec. 39-30. - Applications.](#)

[Sec. 39-31. - Issuance.](#)

[Sec. 39-32. - Vending prohibited in certain locations.](#)

[Sec. 39-33. - Limitations within the Downtown Miami special vending district.](#)

[Sec. 39-34. - Limitations within the Coconut Grove special vending district.](#)

[Sec. 39-35. - Limitations within the Civic Center special vending district.](#)

[Sec. 39-36. - Limitations within restaurant arcade vending zones.](#)

[Sec. 39-37. - Limitations within Miami Arena special vending district.](#)

[Sec. 39-37.1. - Limitations within Biscayne Boulevard special vending district.](#)

[Sec. 39-38. - Prohibited conduct.](#)

[Sec. 39-39. - Open flame cooking.](#)

[Sec. 39-40. - Open flame use.](#)

[Sec. 39-41. - Size requirements for vending stands.](#)

[Sec. 39-42. - Health and sanitation requirements for food vending.](#)

[Sec. 39-43. - Safety requirements.](#)

[Sec. 39-44. - Advertising.](#)

[Sec. 39-45. - Renewal.](#)

[Sec. 39-46. - Denial, suspension, revocation.](#)

[Sec. 39-47. - Notice on premises that uninvited vendors, solicitors, peddlers, etc., are not wanted.](#)

[Sec. 39-48. - Exemptions as to farm products.](#)

[Sec. 39-49. - Exemptions for vendors who exclusively vend written matter.](#)

[Sec. 39-50. - Penalty.](#)

[Sec. 39-51. - Violation a nuisance; summary abatement.](#)

[Sec. 39-52. - Enforcement of article.](#)

### Sec. 39-26. - Definitions.

For the purposes of this Article:

*Biscayne Boulevard special vending district* is defined as all public rights-of-way within that area bounded on the east by the centerline of Biscayne Boulevard; on the north by Northeast 11th Street; on the west by Northeast 1st Avenue; and on the south by Northeast 5th Street.

*Business tax receipt (BTR)* as defined in [Chapter 31](#) of the City of Miami Code.

*Civic center special vending district* is defined as all public rights-of-way within that area bound by and including both sides of Northwest 12th Avenue on the east, Northwest 14th Street on the north, Northwest 12th Street on the south, and Northwest 14th Avenue on the west.

*Coconut Grove special vending district* is defined as all public rights-of-way within that area known as the "Coconut Grove Village Center" which is generally delineated by the SD-2 district zoning boundaries of the city zoning ordinance, as amended, and more particularly described as the area bounded by a line

which marks its point of beginning at the intersection of South Bayshore Drive and Mary Street. From said point of beginning move north on Mary Street to Oak Avenue, then west on Oak Avenue to Matilda Street, then south on Matilda Street to Florida Avenue, then west on Florida Avenue to Margaret Street, then south on Margaret Street to William Avenue, then follow an imaginary straight line extending Margaret Street due south until it intersects with Main Highway, then follow Main Highway north to McFarlane Road, then southeast on McFarlane Road to South Bayshore Drive, then northeast on South Bayshore Drive to Mary Street, which is the point of beginning.

*Department of health* is defined as the Dade County department of public health.

*DDA* is defined as being the Downtown Development Authority of the City of Miami.

*Director* is defined as the director of the department of public works.

*Downtown Miami special vending district* is defined as all public rights-of-way within that area generally commensurate with the boundaries of the Miami Downtown Development Authority, but more specifically described as that area bounded on the east by Biscayne Bay, except between Northeast 17th Street and Northeast 24th Street; on the north by the commercial corridors along Biscayne Boulevard from Northeast 17th Street to Northeast 24th Street; on the west by the Florida East Coast Railway from Northwest 17th Street, Northwest Fifth Street, then west along Northwest Fifth Street to Northwest Third Avenue to West Flagler Street, then west along Flagler Street to the Miami River, then east to the Metrorail guideway; and on the south by Southeast 15th Road; but shall exclude the area comprising the Miami Arena Special Vending District. Said district shall be subdivided into three areas for purposes of awarding franchises and setting franchise fees: area A, which shall consist of Flagler Street between Biscayne Bay and the Miami River; area B, which shall consist of Northeast/Northwest First Street and Southeast/Southwest 1st Street between Biscayne Bay and the Miami River; and area C, which shall include those areas north and south of areas B as follows: the northern segment of area C shall consist of that area bounded on the south by Northeast/Northwest Second Street, on the North by Northeast/Northwest 24th Street, on the west by the Miami River and on the east by Biscayne Bay, but shall not include the area comprising the Miami Arena Special Vending District; the southern segment of area C shall consist of that area bounded on the North by Southeast/Southwest Second Street, on the east by Biscayne Bay, on the west by the Miami River and Southwest Third Street, and on the south by Southeast/Southwest 15th Road.

*Executive director* is defined as the executive director of the Downtown Development Authority of the City of Miami.

*Extended sidewalk* is defined as sidewalk either at an intersection or midblock which has been approximately doubled in width to occupy a former parking lane.

*Food* is defined as solid food and beverages allowed to be sold in accordance with this article.

*Franchise* is defined as the exclusive right to vend in a special vending district pursuant to the provisions of sections [39-33](#), [39-34](#), and [39-37.1](#).

*Franchise document* or *franchise permit* is defined as a document provided by the executive director or director to evidence the right granted pursuant to sections [39-33](#), [39-34](#), and [39-37.1](#) to exclusively vend in a specified vending zone.

*Franchise period* is defined as the time, which shall be one year, (except for the inaugural franchise period for the Biscayne Boulevard special vending district, which shall be until September 30, 2001), a vendor may be granted the franchise for a specific vending zone.

*Licensee* is defined as any person or business entity which has been issued or controls one or more licenses to conduct vending activity in the city.

*Miami Arena special vending district* is defined as all public rights-of-way within that area bounded by the north side of Northeast/Northwest Fifth Street on the south, both sides, respectively of Northwest Third Avenue on the west, Northeast Second Avenue on the east and Northeast/Northwest Tenth Street on the north.

*Motor vehicle* is defined as any vehicle used for the displaying, storing, or transporting of articles offered for sale by a vendor, which is required to be licensed and registered by the department of highway safety and motor vehicles.

*Open flame* is defined as being a heat source which consists of a visible flame or which produces smoke at any time.

*Open flame cooking* is defined as the cooking of food utilizing a heat source which consists of a visible flame or which produces smoke during the cooking process.

*Permittee* is defined as the recipient of a restaurant arcade vending zone permit under the terms and provisions of this article.

*Person* is defined as any natural individual, firm, trust, partnership, association, or corporation, in his or its own capacity or as administrator, conservator, executor, trustee, receiver, or other representative appointed by a court. Whenever the word "person" is used in any section of this article prescribing a penalty or fine as applied to partnerships or associations, the word shall include the partners (both general and limited) or members thereof, and such word as applied to corporations shall include the officers, agents, or employees thereof who are responsible for any violation of said section.

*Planning sticker* is defined as the sticker issued by the planning, building and zoning department pursuant to [section 39-34\(7\)](#).

*Posted notice lottery* is defined as a lottery with notice to be given solely by the posting of at least four signs in each of the city's special and restricted zoning districts, with the exception of the arcade and Miami Arena vending districts, at least 30 days prior to the lottery date.

*Pushcart* is defined as a wheeled vehicle propelled solely by a single human.

*Qualified vendor* is defined as any vendor who successfully completes prequalification of his, her or its application for a vending zone; including pushcart certification and proof of all required licenses and permits.

*Restaurant arcade* is defined as a second-level structure authorized, pursuant to [section 54-186](#) of this Code, to extend within the public right-of-way by revocable permit, which is elevated over a portion of the public sidewalk, and which at the second level contains only seating for a restaurant located within the second floor of an adjacent building.

*Restaurant arcade vending zone* is defined as the ground level public right-of-way sidewalk area under a restaurant arcade, and shall include any widened area of such sidewalk which may extend beyond and parallel to the street side of such restaurant arcade.

*Right-of-way* is defined as land dedicated, deeded, used or to be used for a street, alley, walkway, boulevard, drainage facility, access for ingress or egress, or other purpose by the public, certain designated individuals of governing bodies.

*Stand* is defined as any table, showcase, bench, rack, pushcart, or any other wheeled vehicle or device which may be moved without the assistance of a motor and which is not required to be licensed and registered by the department of highway safety and motor vehicles, used for displaying, storing, or transporting of articles offered for sale by a vendor.

*Street* as used herein includes any primary accessway such as a street, road, lane, highway, avenue, boulevard, parkway, circle, court, terrace, place, or cul-de-sac, and also includes all of the land lying between the right-of-way lines as delineated on a plat showing such streets, whether improved or unimproved.

*Vending* is defined as the act of selling, offering for sale, transferring, or offering to transfer food, merchandise or services to another for pecuniary gain.

*Vending year* is defined as the one-year calendar period from October 1 to September 30.

*Vending zone* is defined as a rectangular area within a restricted vending district where vending is permitted pursuant to this article; said vending zone to be delineated by markings on the sidewalk delineating a rectangle within the limits of which a vending pushcart may be placed.

*Vendor* is defined as any person engaged in the selling, or offering for sale, of food, beverages, services, or merchandise on the public streets, or sidewalks from a stand or motor vehicle or from his person.

*Vendor location* is defined as a sidewalk area, within a vending zone, which has been selected and identified by the public works department as the specific vendor site(s) at which all vending in that zone shall occur.

*Wholesale peddler* is defined as any person who sells or offers for sale any goods, wares, or merchandise to any person engaged in the business of selling at retail in the city, or to any person for the purpose of resale within the city, or to any drugstore, soda fountain, restaurant, cafeteria, hotel, club or tearoom within the city, from a wagon, truck, auto, pushcart or by any other means, operating in or upon the streets of the city in other than a licensed place of business. Such term shall not apply to a wholesale automobile accessories dealer.

*Written matter* is defined as newspapers, periodicals, books, pamphlets or other similar written matter.

(Ord. No. 9880, § 1, 9-13-84; Ord. No. 10045, § 1, 9-26-85; Ord. No. 10479, § 1, 9-8-88; Ord. No. 10499, § 1, 10-27-88; Ord. No. 10660, § 1, 10-12-89; Ord. No. 10855, § 1, 3-14-91; Ord. No. 10891, § 1, 6-20-91; Ord. No. 11169, § 2, 7-26-94; Ord. No. 11212, § 3(39-11), 1-12-95; Ord. No. 11249, § 2, 4-27-95; Code 1980, § 39-11; Ord. No. 12002, § 2, 12-14-00; Ord. No. 13105, § 2, 10-8-09)

### **Sec. 39-27. - Intent of article.**

The intent of this article is to regulate vending on streets, rights-of-way and publicly owned parking facilities within the corporate limits of the city.

(Ord. No. 10891, § 1, 6-20-91; Code 1980, § 39-11.1)

### **Sec. 39-28. - BTR required.**

It shall be unlawful to sell, or offer for sale, any food, beverage, service or merchandise on any street, alley, sidewalk, or public park within the city from any wagon, truck, auto, pushcart, vehicle or by any other means upon the streets, sidewalks, or alleys of the city until the proper BTR has been issued by the department of finance, at which time a metal or plastic tag shall be furnished, upon which tag shall be the words describing the kind of vendor, and the year for which the BTR is paid. Such tag shall be, at all times during the period for which the BTR is paid, securely affixed and attached in a conspicuous place on the left side and upon the stand, wagon, truck, auto, pushcart, or other vehicle used in the business by the vendor or wholesale peddler.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-12; Ord. No. 13105, § 2, 10-8-09)

**Editor's note—**

Ord. No. 13105, § 2, adopted Oct. 8, 2009, changed the title of [§ 39-28](#) from "License required" to "BTR required." The historical notation has been preserved for reference purposes.

**Charter reference—** *Authority of city to license, regulate peddlers, § 3(gg).*

**City Code cross reference—** License fees for peddlers, [§ 31-50](#)

**Sec. 39-29. - License not applicable in certain areas of the city during certain time periods.**

BTR issued under the provisions of [chapter 31](#) to vendors shall not be applicable within certain areas of the city designated by the city manager during specific time periods designated for authorized special events. The areas so designated shall not encompass more than five percent of the total land area of the city; the total of the time periods so specified shall not exceed 30 days in any fiscal year.

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-13; Ord. No. 13105, § 2, 10-8-09)*

**Sec. 39-30. - Applications.**

The BTR required by [section 39-28](#) shall be issued in accordance with [chapter 31](#), of the City Code. The initial application for a vendor's BTR shall include, in addition to the information required in [section 31-35](#):

- (1) Name, home and business address of the applicant and the name and address of the owner, if other than the applicant, of the vending business, stand, or motor vehicle to be used in the operation of the vending business.
- (2) A description of the type of food, service, or merchandise to be sold.
- (3) A description and photograph of any stand or motor vehicle to be used in the operation of the business, including the license and registration number of any motor vehicle used in the operation of the business. Photograph shall be of standard motor vehicle in operational mode.
- (4) Three two-inch by two-inch prints of a full-face photograph, taken not more than 30 days prior to the date of the application, of any person who will sell, or offer for sale, any food, service, or merchandise on any street or sidewalk within the city.
- (5) A certificate of inspection, as required by [section 39-42](#)

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-14; Ord. No. 13105, § 2, 10-8-09)*

**Sec. 39-31. - Issuance.**

Not later than 30 days after the filing of a completed application for a vendor's license, the applicant shall be notified by the finance department for the decision on the issuance or denial of the BTR. Failure of the finance department to place notification of said decision in the mail or personally notify the applicant with acknowledgment shall require immediate issuance of the requested license to the applicant. The public works director or designee shall consider the standards set forth in sections [39-32](#) through [39-43](#), in determining whether to recommend to the finance director or designee that a BTR be issued. If the issuance of the BTR is approved, the finance department shall issue the BTR. If the BTR is denied, the applicant shall be provided with a statement of the reasons therefor, which reasons shall be entered in writing on the application. The applicant shall be entitled to a hearing, pursuant to [section 39-46](#). A BTR issued pursuant to this action is valid for a period as prescribed in [section 31-37](#).

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-15; Ord. No. 13105, § 2, 10-8-09)*

**Sec. 39-32. - Vending prohibited in certain locations.** 

Vending is prohibited in the following locations:

- (1) Within special vending districts or restaurant arcade vending zones, except within designated vending zones of said areas.
- (2) From a public parking lot, metered or unmetered parking space, on-street parking space, or loading zone.
- (3) Within 500 feet of any property used for school purposes (preschool, elementary, secondary) on all school days between the hours of 7:00 a.m. and 4:30 p.m. [115]
- (4) On any combination sidewalk and curb width less than six feet in width.
- (5) Within five feet of the entranceway to any building.
- (6) Within 100 feet of any driveway entrance to a police or fire station, or within 20 feet of any other driveway.
- (7) Within 20 feet of any bus stop zone.
- (8) Within five feet of the pedestrian crosswalk at any intersection, or designated pedestrian crossing point.
- (9) Within ten feet of any handicapped parking space, or access ramp.
- (10) Within 20 feet of a sidewalk cafe permitted pursuant to chapter 54 of the city Code.

*(Ord. No. 9880, § 1, 9-13-84; Ord. No. 10045, § 1, 9-26-85; Ord. No. 10499, § 1, 10-27-88; Ord. No. 10660, § 1, 10-12-89; Ord. No. 10891, § 1, 6-20-91; Ord. No. 11212, § 3(39-16), 1-12-95; Code 1980, § 39-16)*

**Sec. 39-33. - Limitations within the Downtown Miami special vending district.** 

Vending within the Downtown Miami vending district shall be subject to all generally applicable rules and regulations in this article except as contrarily and specifically provided below:

- (1) No merchandise shall be vended or displayed other than:
  - a. Prepackaged foods, as defined by 61C-4.009, Florida Administrative Code (1994), as amended, of the snack food type.
  - b. Prepared foods including, but not limited to: ice cream, baked goods, fresh fruit and the like.
  - c. Unprepared foods including, but not limited to: hot dogs, crepes and the like.
  - d. Plants and flowers including, but not limited to: fresh cut or dried flowers or potted plants and the like.
- (2) Vending of merchandise shall be prohibited from any type of vehicle or stand other than a pushcart of the specific types and construction shown and described on composite "exhibit B," attached to Ordinance No. 11212. Pushcarts satisfying said criteria may be purchased by the DDA utilizing fees collected from vending zone franchises and may be leased to the franchisees at lease rates to be determined by the DDA. Vendors shall not be precluded from using non-DDA provided equipment or pushcarts. However, said materials shall satisfy the above criteria and be inspected and certified by DDA as having complied with this section.
- (3) No merchandise, supplies, containers or any other items related to the vendor shall be placed anywhere within the public right-of-way other than on or concealed within the pushcart, with the exception of one folding chair or wooden stool of a type approved by the DDA.
- (4) No vendor or entity shall own, operate, hold or control a local business tax receipt for more than one pushcart in the herein district.
- (5) Vending zones.
  - a. Assignment of vendors to specific vending zones.
    1. Franchise rights.





4. Vending zones may also be eliminated.
  5. Eliminations or substitutions shall be based on findings by the executive director or director that such action is warranted on health and safety grounds, or necessitated by rights-of-way improvement or private or public construction activity.
- c. Lottery.
1. The DDA shall establish and the executive director shall supervise a lottery system whereby those persons possessing, as conditions precedent to participating in the lottery, valid and appropriate state licenses (upon required inspections, from the state department of business and professional regulation for the sale of prepared food, and/or the state department of agriculture for the sale of prepackaged food, or their successor agencies), an local business tax receipt, appropriate state and local sales tax certificates and DDA pushcart certification shall be publicly chosen by chance for vending zones in this district. The executive director or downtown NET administrator shall assign each vending zone a number corresponding to a location on the appropriate vending map. All qualified vendors shall have their names placed into containers for a public drawing by the executive director or his or her designee to determine which location shall serve as the vending zone for each vendor for the franchise period. At the conclusion of the franchise period all franchise rights shall end and all franchises shall be subject to a new lottery.
  2. The DDA is authorized and directed to annually issue a "Notice of Street Vending Franchise Opportunities in Downtown Miami." Said notice for each franchise period shall be publicly advertised in a newspaper of general circulation approximately 60 days prior to each franchise period and shall indicate the pending availability of exclusive vending zones in the district, and the terms of such availability, including the date, place and time of the lottery. Notices as for a posted notice lottery may also be given, but shall be considered courtesy notice only.
  3. Utilizing the standards and criteria set forth in this article, the DDA may promulgate such reasonable supplementary rules, regulations and/or procedures as are necessary to implement and effectuate the herein lottery and vending zone assignment process, which shall include participation by a representative of the Downtown Miami Partnership. Said supplementary rules, regulations and procedures shall be filed with the city clerk, and also made available at the DDA and the downtown NET office.
  4. For vending zones which may become available during the franchise period due to vacancy, abandonment or executive director's or director's action, the executive director may specify the date, time and place for the holding of a special lottery for such designated vending zone(s), and shall publicly advertise said information as for a posted notice lottery.
  5. All franchise documents are nontransferable. Sale of a majority of stock in a corporate franchise by stockholders listed on the franchise application or sale of a majority interest in a partnership as listed on the franchise application shall be deemed a transfer of the franchise, which is prohibited. The franchise document shall be in the possession of the vendor and immediately accessible at all times, and shall be displayed to a police officer, code enforcement officer or Downtown Miami Neighborhood Enhancement Team ("NET") official upon request. Failure to immediately provide this document, along with a valid local business tax receipt, the pushcart certification required by subsection (2) of this section, sales tax certificate(s) required by subsection (16) of this section, and appropriate current

- state inspection license(s) shall be grounds for immediate removal of the pushcart from the vending zone and district, suspension of the franchise and initiation of local business tax receipt and franchise revocation proceedings by the executive director or NET administrator.
6. Franchises awarded pursuant to this section shall be subject to [section 39-29](#). Furthermore, the award of a franchise pursuant to this section does not grant or infer vested rights to the use of the public rights-of-way by the franchisee.
  7. Any vending zone or franchise document issued pursuant to this section shall be subject to modification by ordinance at any time deemed necessary by the city commission. Vending in any vending zone may be temporarily suspended or relocated by the director upon reasonable notice when private or public construction or activities or health and safety concerns of the director make it unsafe or impractical to allow vending in that vending zone. Such suspension(s) which last for a continuous or cumulative period in excess of five days of a franchise period shall result in a pro rata refund of the lottery franchise fee paid by the franchisee who is the subject of such suspension. No other payments or compensation shall be owed by the city or due the franchisee as a result of such suspension(s). A vendor so dispossessed may, if possible, be offered a substitute vending zone by the executive director without the necessity of lottery proceedings. Said new location shall be valid for the balance of the time remaining on the vendor's franchise document for that franchise period, or until the vendor's original franchise is again available, whichever date or event occurs first. If a substitute location is accepted by the vendor the refund shall be only for the actual days of suspended operation, and shall not include the assigned day(s) of operation in the substitute location.
  8. Vending activity voluntarily terminated, or suspended or revoked due to unauthorized absence or other violations of this article or otherwise violating the Code of the City of Miami, Dade County or general law shall not be the basis for any pro rata refund of a franchise fee. Revocation of franchise documents based on voluntary termination, unauthorized absences or violations shall result in a forfeiture of the entire franchise fee.
- d. Limitations within vending zones.
1. There shall be no more than one vendor permitted to operate within each vending zone.
  2. Each vendor shall be permitted to operate within only one vending zone.
  3. Each vending zone shall approximate the size of the specific pushcart permitted within said vending zone and shall be clearly marked on the sidewalk.
  4. Vending pushcarts shall be, at all times, positioned so that their longest side is parallel to the street curb.
- e. All participants in lottery proceedings pursuant to this section shall submit, as a condition precedent to participating, a copy of an appropriate valid local business tax receipt, certification from the DDA that the pushcart which is to be used in this district has been issued a document evidencing compliance pursuant to subsection (2) of this section, sales tax certification pursuant to subsection (16) of this section and the appropriate state license pursuant to subsection (20) of this section.
- f. Unauthorized absence from a designated vending zone shall constitute a basis for suspension and revocation of a franchise document. Upon certification by the executive director or NET administrator that a vending zone has been unoccupied for a continuous period of 15 days for reasons other than those mentioned in subsection (5)c.5 of this section or [section 39-29](#), the executive director or NET administrator shall notify the vendor of the intent to revoke the vendor's franchise unless clear

evidence of vending activity during the 15-day period in question is provided to the executive director or NET administrator. Subsequent to ten-day notice mailed by certified mail to the address shown on the vendor's lottery application form, the executive director shall conduct a hearing and may revoke the vending franchise and reward the franchise to a different vendor, pursuant to a posted notice lottery, for the balance of that franchise period. The vendor subject to such revocation may appeal said decision in the same manner provided in [section 54-230](#). An appeal shall not stay an order banishing a pushcart or franchisee.

- g. Any franchisee incurring three written notices of violation of this article within a two-year period shall be the subject of the following franchise revocation proceedings:
    1. When violations occur, the franchisee shall be notified by the executive director, his designee, or downtown NET office in person or via certified mail. The first violation notice or citation shall be a reprimand; the second violation notice or citation shall be a warning; the third violation notice or citation shall result in an automatic revocation of franchise document, immediate removal of the franchisee's pushcart from the district, and banishment of the violator from the district for a period of one calendar year.
    2. Revocations may be appealed in the same manner provided in [section 54-230](#). An appeal shall not stay an order to remove a pushcart or banish a franchisee from the district.
  - h. A franchisee may voluntarily relinquish a franchise through written, notarized notification to the executive director, specifying an effective date. On said date the subject vending zone shall be automatically reclassified as vacant, and subject to reassignment in a special lottery. The relinquishing franchisee shall be ineligible to participate in any lottery in that specific special vending district for the balance of that franchise period.
- (6) All goods for sale other than those on display must be stored within the structure of the pushcart and shall not be visible to the general public.
  - (7) It shall be unlawful for any vendor to use any noise making device to solicit customers.
  - (8) Pushcarts shall not be chained or otherwise affixed to trees, lightpoles, sign stanchions or any other object in the right-of-way.
  - (9) Pushcarts shall be required to be in their vending zone between the hours of 9:00 a.m. and 6:00 p.m. on a weekday and between the hours of 10:00 a.m. and 6:00 p.m. on a Saturday or Sunday.
  - (10) Vending shall be prohibited within eight feet of the entranceway to any building, and within 50 feet of the entranceway to any church, synagogue or other place of worship.
  - (11) No open flame cooking shall be permitted.
  - (12) Vending zones shall not be occupied exclusively by a selected vendor pursuant to this section until July 1, 1995. Said date shall initiate the inaugural franchise period for the Downtown Miami special vending district.
  - (13) Fees collected under this subsection are for franchises granted for the exclusive right to use a portion of the public right-of-way, and are in addition to other permit fees and local business taxes imposed by law.
  - (14) All franchise fees collected pursuant to this section shall be placed in a special account established for the Downtown Miami special vending district by the City of Miami's director of finance, and shall be utilized exclusively by the executive director, upon approval of the DDA board of directors, for the administration of this district, its management services and purchase or replacement of pushcarts and/or related equipment.
  - (15) The executive director shall design and distribute to those awarded a vending zone a franchise document identifying the person or entity chosen by lottery, the specific location

- where said person or entity is to be allowed to vend exclusively during the vending period, and the duration of such entitlement.
- (16) Except as otherwise provided in this section all franchise documents issued for vending activity within the district shall be valid for a period of one year or, in the case of special lottery franchisees, the balance of the franchise period. Prior to the expiration date (September 30 of each year), vending zones shall once again be awarded pursuant to the lottery requirements of this section. The reallocation and assignment of vending zones shall become effective on October 1 of each year and no vendor shall be allowed to occupy the same vending zone for two consecutive franchise periods.
- (17) All franchise documents issued for vending activity in this district shall only be valid during one franchise period, and shall expire on the expiration date shown on the franchise document and records of the executive director. Upon such expiration the vendor's exclusive right to such vending zone shall terminate, and vending rotation rights shall once again be awarded pursuant to the lottery procedures of this section.
- (18) Liability and insurance.
- a. Prior to the issuance of a franchise document, the vendor shall furnish the executive director with a signed statement that said vendor shall hold harmless and indemnify the city and DDA and their officers and employees for any claims for damages to property or injury to persons which may be occasioned by any activity carried on under the terms of the franchise document and associated local business tax receipt.
- b. Prior to the issuance of a franchise document, said vendor shall also furnish proof of and maintain such public liability and property damage from all claims and damage to property or bodily injury, including death, which may arise from or in connection with operations under the franchise document and associated local business tax receipt. Such insurance shall provide coverage of not less than \$500,000.00 for bodily injury, and property damage respectively per occurrence. Such insurance shall be without prejudice to coverage otherwise existing and shall name as additional insured the city and DDA and their officers and employees, and shall further provide that the policy shall not terminate or be canceled for any reason, prior to the completion of the franchise period without 45 days' written notice to the risk management division of the department of fire-rescue or its successor, the executive director and the director of public works of the city at the addresses shown in the franchise document.
- (19) Sales tax certification. Prior to the issuance of a franchise document, the vendor shall also furnish original evidence of a valid certificate of resale or equivalent document from the Florida Department of Revenue and Metropolitan Dade County, if applicable, evidencing that the vendor and the specific vending activity authorized by said franchise document have been permitted by said tax collection entities to the extent mandated by law. Franchisee(s) shall furnish upon demand, evidence that the herein requested certificate of resale or equivalent document is current. Failure to maintain said certification shall constitute a basis for suspension and/or revocation of a franchise document.
- (20) State license inspection and certification. Prior to issuance of a franchise document, the vendor shall also furnish original evidence of a valid license issued, upon inspection, by the state department of business and professional regulation (for vending prepared food, as defined by state regulations) and/or the state department of agriculture (for vending prepackaged food, as defined by state regulations).

*(Ord. No. 9880, § 1, 9-13-84; Ord. No. 10479, § 1, 9-8-88; Ord. No. 10633, § 1, 9-14-89; Ord. No. 10805, § 1, 10-25-90; Ord. No. 10891, § 1, 6-20-91; Ord. No. 11212, § 3(39-17), 1-12-95; Ord. No. 11249, § 2, 4-27-95; Code 1980, § 39-17; Ord. No. 11288, § 2, 7-13-95; Ord. No. 12885, § 1, 2-8-07)*

## **Sec. 39-34. - Limitations within the Coconut Grove special vending district.**

Vending within the Coconut Grove special vending district shall be subject to all generally applicable rules and regulations in this article, including [section 39-33](#), except as contrarily and specifically provided below:

- (1) No merchandise shall be vended or displayed other than:
  - a. Handmade art and crafts: Any handmade art or craft which takes a material which has been changed into an entirely different shape, design, form or function is acceptable as an original object of art or craft. The craft or art object of sale must be predominantly created or altered in form by the street artist or craftsperson. Assembly alone does not constitute handmade.
  - b. Plants and flowers: Nonhazardous or noncontrolled vegetation limited to fresh cut or dried flowers or potted plants.
- (2) Vending of merchandise shall be prohibited from any type of vehicle or stand other than a pushcart of the type shown on attachment A hereto (not reproduced in the Code). No merchandise, supplies, containers, or other items related to the vendor shall be placed anywhere in the public right-of-way other than in or on the pushcart except for one folding armchair or wooden stool. No vendor shall operate or hold an local business tax receipt for more than one pushcart in the herein district.
- (3) Vending zones.
  - a. Quantity and location of vending zones. The number of vending zones shall not exceed ten. No vending shall be permitted in the Coconut Grove special vending district except within the sidewalk areas specifically designated on the official graphic attached hereto as "attachment A," as amended, and herein referred to as the "vending map." (Attachment A is not reproduced in the Code.) Substitute locations may be approved by the director of the department of public works upon a finding that such new vending zone(s) is in an unobstructed sidewalk area, and otherwise satisfies all provisions of this article and other applicable regulations. Such substitutions shall be based on findings by the director that such temporary or permanent relocation is warranted on health and safety grounds, or necessitated by rights-of-way improvement or private or public construction activity. This vending map, as amended, shall be the official vending zone locator for the district, and shall be kept in the office of the director, with copies furnished upon its adoption, and upon any amendment thereto, to the city clerk and the Coconut Grove Neighborhood Enhancement Team (NET) office.
  - b. Limitations within vending zones.
    1. There shall be no more than one vendor permitted to operate from each vending zone. Each vendor shall be permitted to operate from only one vending zone.
    2. Each vending zone shall approximate the size of one permitted pushcart and shall be clearly marked on the sidewalk by the department of public works.
    3. Vending pushcarts shall be at all times situated in a position with their longest side parallel to the street curb.
  - c. Assignment of vendors to specific vending zones.
    1. Franchise rights. Vending zones within this district shall be occupied only by licensed vendors willing to pay the city for the franchise right to vend exclusively from designated vending zones in the Coconut Grove special vending district, subject to applicable rules, regulations, ordinances and statutes governing vending. There shall be a franchise fee due of \$200.00 per month, for a total of \$1,200.00 per franchise period, for franchises. As a condition precedent to receiving a franchise, the total amount due for the franchise period shall be paid in full. Payment shall be by cashier's check, bank certified funds, or money order payable to the city. Failure to tender required payment on the date of the lottery shall invalidate such award and vacate the vending zone.

2. Lottery.
  - i. The director shall establish and supervise a lottery system whereby those persons possessing a valid and appropriate local business tax receipt, appropriate state and local sales tax certificate(s), and planning sticker to vend shall be chosen by chance for vending zones in this district. The director or NET administrator shall assign each vending zone a sequential number corresponding to a clockwise circuit pattern of sequential locations on the vending map. All qualified vendors shall have their names placed into a container for a drawing by the director or NET administrator to determine which location shall serve as the initial vending zone for each vendor at the beginning of a franchise period. On the first day of each month following the first month of each franchise period all vendors shall relocate, via rotation, to the next vending zone in the aforementioned sequence. All franchise rights shall transfer to the new location and cease in the prior location upon such rotation. Said rotation shall continue for the duration of the franchise period. At the conclusion of the franchise period all franchises shall be subject to a new lottery.
  - ii. The director is authorized to issue a "notice of street vending franchise opportunities in Coconut Grove." Said notice for each franchise period shall be publicly advertised in a newspaper of general circulation in approximately mid-August and mid-February of each calendar year, and shall indicate the pending availability of exclusive vending zones in the district and the terms of such availability, including the date, place and time of the lottery. Notices as for a posted notice lottery may also be given, but shall be considered courtesy notice only.
  - iii. Utilizing the standards and criteria set forth in this article, the director may promulgate such reasonable supplementary rules, regulations and procedures as are necessary to implement and effectuate the herein lottery and vending zone assignment process.
  - iv. For vending zones which may become available during the franchise period due to abandonment or director's action, the director shall specify the date, time and place for the holding of a special lottery for such designated vending zone(s), and shall publicly advertise said information as for a posted notice lottery.
  - v. All franchise documents are nontransferable. Sale of a majority of stock in a corporate franchise by stockholders listed on the franchise application or sale of a majority interest in a partnership as listed on the franchise application shall be deemed a transfer of the franchise, which is prohibited. The franchise document shall be in the possession of the vendor at all times and shall be displayed to a police officer, Code enforcement officer or Coconut Grove Neighborhood Enhancement Team (NET) official upon request. Failure to provide this document, along with a valid local business tax receipt, the planning, building and zoning department sticker required by subsection (7), and sales tax certificate(s) required by subsection (14), shall be grounds for immediate removal of the pushcart from the vending zone and district, suspension of the franchise and initiation of local business tax receipt and franchise revocation proceedings by the director or NET administrator.
  - vi. Franchises awarded pursuant to this section shall be subject to [section 39-29](#). Furthermore, the award of a franchise pursuant to this section does not grant or infer vested rights to the use of the public rights-of-way

- by the franchisee.
- vii. Any vending zone or franchise document issued pursuant to this section shall be subject to modification by ordinance at any time deemed necessary by the city commission. Vending in any vending zone may be temporarily suspended or relocated by the director upon reasonable notice when private or public construction or activities or health and safety concerns of the director make it unsafe or impractical to allow vending in that vending zone. Such suspension(s) which lasts for a continuous or cumulative period in excess of five days of a franchise period shall result in a pro rata refund of the lottery franchise fee paid by the franchisee who is the subject of such suspension. No other payments or compensation shall be owed by the city or due the franchisee as a result of such suspension(s). A vendor so dispossessed may, if possible, be offered a substitute vending zone by the director without the necessity of lottery proceedings. Said new location shall be valid for the balance of the time remaining on the vendor's franchise document for that franchise period, or until the vendor's original franchise is again available. If a substitute location is accepted by the vendor the refund shall be only for the actual days of suspended operation, and shall not include the day(s) of operation in the substitute location.
- viii. Vending activity suspended pursuant to [section 39-38](#) or revoked due to unauthorized absence or violations of the codes of the city, county or general law shall not be the basis for any pro rata refund of a franchise fee. Contrarily, revocation of franchise documents based on unauthorized absences or violations shall result in a forfeiture of the entire franchise fee.
- d. All participants in lottery proceedings pursuant to this section shall submit, as a condition precedent to participating, a copy of an appropriate valid local business tax receipt, certification from the planning, building and zoning department that the pushcart which will be used in this district has been issued a planning sticker pursuant to subsection (7), and sales tax certification pursuant to subsection (14).
- e. Unauthorized absence from a designated vending zone shall constitute a basis for suspension and revocation of a franchise document. Upon certification by the director or NET administrator that a vending zone has been unoccupied for a continuous period of 15 days for reasons other than those mentioned in subsection (3)c.2.vi or [section 39-29](#), the director or NET administrator shall notify the vendor of the intent to revoke the vendor's franchise unless clear evidence of proof of vending activity during the 15-day period in question is provided to the director. Subsequent to ten-day notice mailed by certified mail to the address shown on the vendor's lottery application form, the director or NET administrator shall conduct a hearing and may revoke the vending franchise and reward the franchise to a different vendor, pursuant to a posted notice lottery, for the balance of that franchise period. The vendor subject to such revocation may appeal the director's decision in the same manner provided in [section 54-230](#)
- f. Any franchise incurring three written notices of violation of this article shall be the subject of the following franchise revocation proceedings:
1. When violations occur, the franchisee shall be notified by the director of Coconut Grove NET office in person or via certified mail. The first violation notice or citation shall be a reprimand; the second violation notice or citation shall be a warning; the third violation notice or citation shall result in an automatic revocation of franchise document, immediate removal of the franchisee's pushcart from the district, and banishment of the violator from the



- district for a period of one calendar year.
2. Revocations may be appealed in the same manner provided in [section 54-230](#). An appeal shall not stay an order by the director or NET office to remove a pushcart from the district.
- (4) All goods for sale other than those on display must be stored within the structure of the pushcart and shall not be visible to the general public.
- (5) It shall be unlawful for any vendor to use any noise-making device to solicit customers.
- (6) Vending pushcarts may not be chained or otherwise affixed to trees, light poles, sign stanchions or other stationary entities on the sidewalk.
- (7) The design and dimension for the pushcart shall be substantially in conformance with the drawing, which is attached hereto as attachment A (on file with the city). Additionally, all pushcarts shall bear a sticker from the city planning, building and zoning department indicating that the pushcart has been reviewed by it and satisfies the following design guidelines:
- a. Each pushcart must have a minimum of two wheels.
  - b. No pushcart may have more than four wheels.
  - c. Wheels must be functional and decorative. Nonfunctional wheels are prohibited.
  - d. All wheels, except as provided below, shall be made of wood and open-spoked.
  - e. Automobile wheels and tires, or other such obviously out of place wheel designs, are prohibited.
  - f. Casters are prohibited except the use of a caster as a third wheel support for increased mobility of a heavy pushcart.
  - g. Each pushcart must have stability features such as brakes or chocks to fix its location.
  - h. Pushcarts shall be built of durable wood such as oak or similar solid woods.
  - i. Pushcart construction should exhibit thoughtful design and good workmanship.
  - j. Pushcarts must be designed to contain all products, supplies and equipment necessary to their operation.
  - k. Each pushcart must have a canopy which comes out of the body of the cart.
  - l. Flashing or moving lights are not permitted.
  - m. Use of loudspeakers or recorded high volume music is not permitted.
- (8) No pushcart shall be in its designated vending zone before 4:30 p.m. on a weekday, or 10:00 a.m. on a Saturday and Sunday, and except for emergencies, shall not leave its designated vending zone until 2:00 a.m. of the following day. No pushcart is permitted to remain in its vending zone between 2:00 a.m. and 4:30 p.m. of the following weekday or between 2:00 a.m. and 10:00 a.m. on a Saturday or Sunday.
- (9) A vending zone shall not be occupied exclusively by a vendor until October 1, 1994.
- (10) Fees collected under this subsection are declared to be franchise fees charged for the right to exclusive commercial use of a portion of the public rights-of-way in Coconut Grove, and are in addition to local business taxes imposed by law and other permit fees which may be collected to defray the cost of administration of this subsection. All franchise fees collected by the director of finance or his designee pursuant to this section shall be placed in a special account established for the "Coconut Grove festival committee," and shall be used for purposes of making street and sidewalk improvements in the Coconut Grove area under said committee's jurisdiction.
- (11) The director shall design and distribute to those awarded a vending zone a franchise document identifying the person or entity chosen by lottery, the specific location where said person or entity is to be allowed to initially vend exclusively during the vending period, and the duration of such entitlement.
- (12) All franchise documents issued for vending activity in this district shall only be valid during one franchise period, and shall expire on the expiration date shown on the franchise document and

records of the director. Upon such expiration the vendor's exclusive right to such vending zone shall terminate, and vending rotation rights shall once again be awarded pursuant to the lottery procedures of this section.

- (13) Liability and insurance.
- a. Prior to the issuance of a franchise document, the vendor shall furnish the director with a signed statement that said vendor shall hold harmless the city, its officers and employees, and shall indemnify the city, its officers and employees for any claims for damages to property or injury to persons which may be occasioned by any activity carried on under the terms of the franchise document and associated local business tax receipt.
  - b. Prior to the issuance of a franchise document, said vendor shall also furnish and maintain such public liability and property damage from all claims and damage to property or bodily injury, including death, which may arise from operations under the franchise document and associated local business tax receipt or in connection therewith. Such insurance shall provide coverage of not less than \$500,000.00 for bodily injury, and property damage respectively per occurrence. Such insurance shall be without prejudice to coverage otherwise existing therein and shall name as additional insured the city, its officers and employees, and shall further provide that the policy shall not terminate or be cancelled prior to the completion of the franchise period without 45 days' written notice to the risk management division of the department of fire-rescue, and the director of public works of the city at the address shown in the franchise document.
- (14) Sales tax certification. Prior to the issuance of franchise documents, said vendor shall also furnish original evidence of a valid certificate of resale or equivalent document from the Florida department of revenue and Metropolitan Dade County, if applicable, evidencing that said vendor and the specific vending activity authorized by said franchise document have been permitted by said tax collection entities to the extent mandated by law. Franchisee(s) shall furnish, upon demand, evidence that the herein requested certificate of resale or equivalent document is current; and failure to maintain said certification shall constitute a basis for suspension and/or revocation of a franchise document.

*(Ord. No. 10499, § 1, 10-27-88; Ord. No. 11169, § 2, 7-26-94; Code 1980, § 39-17.1; Ord. No. 11288, § 2, 7-13-95; Ord. No. 11800, § 3, 6-8-99; Ord. No. 12885, § 1, 2-8-07)*

### **Sec. 39-35. - Limitations within the Civic Center special vending district.**

Vending within the Civic Center special vending district shall be subject to all rules and regulations in this article, including [section 39-33](#), except as contrarily and specifically provided below:

- (1) No merchandise shall be vended or displayed other than food and fresh cut flowers.
- (2) No licensee shall operate or hold an occupational license for more than one pushcart in the herein regulated district.
- (3) Vending zones.
  - a. Location of vending zones. Vending shall be prohibited in the Civic Center special vending district except within the sidewalk areas generally designated on the graphic attached hereto as "attachment A," which is not reproduced herein. The specific vending locations shall be the responsibility of the department of public works using the standards and criteria contained in this article. Vending zones and vendor locations may be deleted by the director of the department of public works upon a finding that the existence of such zone or location creates an obstruction to pedestrian or vehicular traffic or otherwise creates a threat to the public health, safety, or general welfare. Additional locations may be approved by the director of the department of public works

upon a finding that such vending location is in a generally designated area, and otherwise satisfies all provisions of this article and other applicable regulations.

- b. Limitations within vending zones.
  1. There shall be no more than one vendor permitted to operate from each vending location and such vendor may not move from location to location on the same day.
  2. Each vending location shall approximate the size of one permitted pushcart and shall be clearly marked on the sidewalk by the department of public works.
  3. All vending locations shall be spaced a distance of not less than 50 feet from any other vending location.
- (4) All goods for sale other than those on display must be stored within the structure of the pushcart and shall not be visible to the general public.
- (5) It shall be unlawful for any vendor to use any noise-making device to solicit customers.
- (6) Vending pushcarts may not be chained or otherwise affixed to trees, light poles, sign stanchions or other stationary entities on the sidewalk.
- (7) Vending is prohibited within the herein vending district between the hours of 7:00 p.m. to 7:00 a.m., and pushcarts shall not be located in this district during these hours.
- (8) Open flame cooking shall not be permitted.

(Ord. No. 10660, § 1, 10-12-89; Code 1980, § 39-17.2)

### **Sec. 39-36. - Limitations within restaurant arcade vending zones.**

Vending within a restaurant arcade vending zone shall be subject to all rules and regulations in this article, except as contrarily and specifically provided below:

- (1) *Fee.* The annual permit fee for establishing or maintaining a restaurant arcade vending zone shall be \$20.00 per square foot of usable sidewalk area, as determined by the department of public works. The fee is in addition to the license required pursuant to [section 39-28](#)
- (2) *Permit application.*
  - a. Application for a permit to operate a restaurant arcade vending zone shall be made at the department of public works in a form deemed appropriate by the director. Such application shall include the following information:
    1. Name and address of the applicant;
    2. A copy of a valid permit to operate a restaurant arcade over the sidewalk area which is the subject of the application;
    3. A copy of current liability insurance;
    4. A drawing (minimum scale of one-fourth inch equals one foot) showing the layout and dimensions of the existing sidewalk area and adjacent private property, proposed location, size and number of pushcarts, location of doorways, location of trees, parking meters, bus shelters, sidewalk benches, trash receptacles, and any other sidewalk obstruction either existing or proposed within the pedestrian area; and
    5. Photographs, drawings, or manufacturers' brochures fully describing the appearance of all proposed pushcarts, umbrellas, or other objects related to the restaurant arcade vending zone.
  - b. Applications shall be accompanied by a nonrefundable application fee of \$150.00.
  - c. Applications shall be reviewed by the following departments: public works; planning, building and zoning; fire-rescue; and finance (license division and risk management division).

- d. Within 30 days of receipt of a completed application, the director shall issue a letter of intent to approve or deny the permit.
  - e. The applicant shall provide proof of required insurance prior to receiving the requested permit.
- (3) *Permit requirements.*
- a. No person or entity shall establish a restaurant arcade vending zone on any public sidewalk unless such person or entity has obtained a valid permit to operate that restaurant arcade vending zone in such a manner pursuant to this article.
  - b. Vending activity within any particular restaurant arcade vending zone shall be restricted to individuals or entities shown as the permittee(s) for the corresponding restaurant arcade on a valid revocable permit issued pursuant to [section 54-186](#) of the city Code.
- (4) *Application review standards and criteria.* The following standards and criteria shall be used in reviewing an application for a restaurant arcade vending zone permit:
- a. The area to be considered shall have sidewalks, including extended areas, which are 14 feet in width or greater.
  - b. Restaurant arcade vending zones shall be located in such a manner that a minimum ten-foot-wide clear pedestrian path is maintained at all times. In areas of congested pedestrian activity, the director is authorized to require a wider pedestrian path, as circumstances dictate.
  - c. Umbrellas, canopies and other decorative material shall be fire retardant pressure-treated, or manufactured of fire resistive material.
  - d. Pushcarts shall not exceed four feet in width and six feet in length, exclusive of canopies and umbrellas, which are not required.
  - e. Additionally, all pushcarts shall satisfy the following design guidelines:
    - 1. Each pushcart must have a minimum of two wheels.
    - 2. No pushcart may have more than four wheels.
    - 3. Wheels must be functional and decorative. Nonfunctional wheels are prohibited.
    - 4. Automobile wheels and tires, or other such obviously out of place wheel designs, are prohibited.
    - 5. Casters are prohibited except the use of a caster as a third wheel support for increased mobility of a heavy pushcart.
    - 6. Each pushcart must have stability features such as brakes or chocks to fit its location.
    - 7. Pushcarts shall be built of durable materials.
    - 8. Pushcart construction shall exhibit thoughtful design and good workmanship and aesthetically compliment applicable city master plans or projects for the surrounding area, both to ensure the safety and convenience of users, and to enhance the visual and aesthetic quality of the urban environment. Design, materials, and colors shall be sympathetic and harmonious with an urban environment.
    - 9. Pushcarts must be designed to contain all products, supplies and equipment necessary to their operation.
    - 10. All electrical apparatus on a pushcart should be of a low voltage type. All electrical connections shall be by overhead connection and be of a design and type approved by the director.
- (5) *Liability and insurance.*
- a. Prior to the issuance of a permit, the applicant shall furnish the director with a signed statement, in a form approved by the city attorney, that the permittee shall hold harmless the city, its officers and employees and shall indemnify the city, its officers

and employees for any claims for damages to property or injury to persons which may be occasioned by an activity carried on under the terms of the permit.

- b. Permittee shall furnish and maintain public liability, food products liability, and property damage insurance in an amount sufficient to protect the city from all claims and damage to property or bodily injury, including death, which may arise from operations under the permit or in connection therewith. Such insurance shall provide coverage of not less than \$1,000,000.00 for bodily injury, and property damage, respectively, per occurrence. Such insurance shall be approved by the risk management division of the department of finance, shall be without prejudice to coverage otherwise existing therein and shall name as additional insured the city, its officers and employees, and shall further provide that the policy shall not terminate or be cancelled prior to the completion of the permit period without 45 days' written notice to the risk management division of the department of finance, and the director of public works of the city at the address shown in the permit.
- (6) *Form and condition of permit.* The permit shall be issued on a form deemed suitable to the director. In addition to naming the permittee and any other information deemed appropriate by the director, the permit shall contain the following conditions:
- a. Each permit shall be effective for one year subject to annual renewal.
  - b. The permit issued shall be personal to the permittee only and shall not be transferable in any manner.
  - c. The permit may be suspended by the director when necessary to clear sidewalk areas for a "community or special event" authorized by a permit issued by the police department.
  - d. The director may require the temporary removal of restaurant arcade vending zones when street, sidewalk, or utility repairs necessitate such action.
  - e. The department of public works or the police department may immediately remove or relocate all or parts of the restaurant arcade vending zone in emergency situations.
  - f. The city and its officers and employees shall not be responsible for restaurant arcade zone components relocated during emergencies.
  - g. The permit shall be specifically limited to the area shown on the "exhibit" attached to and made part of the permit.
  - h. The permittee shall use positive action to assure that its use of the sidewalk in no way interferes with sidewalk users or limits their free unobstructed passage.
  - i. The sidewalk area covered by the permit shall be maintained in a neat and orderly appearance at all times and the area shall be cleared of all debris on a periodic basis during the day, and again at the close of each business day.
  - j. No advertising signs or business identification signs shall be permitted in the public right-of-way; this shall not prohibit the use of umbrellas carrying company logotypes.
  - k. The permittee shall notify the director of public works, in writing, when operation of the restaurant arcade vending zone begins. The notice shall be delivered to the director within 24 hours of such commencement.
  - l. The issuance of a restaurant arcade vending zone permit does not grant or infer vested rights to use of the sidewalk area by the permittee. The city retains the right to deny the issuance of a permit or the renewal of a permit.
- (7) *Denial, revocation or suspension of permit; removal and storage fees; emergencies.*
- a. The director may deny, revoke, or suspend a permit for any restaurant arcade vending zone authorized in the city if it is found that:
    1. Any necessary business or health permit has been suspended, revoked, or cancelled.
    - 2.

- The permittee does not have insurance which is correct and effective in the minimum amount described in subsection (5).
3. Changing conditions of pedestrian or vehicular traffic cause congestion necessitating removal of restaurant arcade vending zone. Such decision shall be based upon findings of director that the minimum ten-foot pedestrian path is insufficient under existing circumstances and represents a danger to the health, safety, or general welfare of pedestrians or vehicular traffic.
  4. The permittee has failed to correct violations of this article or conditions of his permit within three days of receipt of the director's notice of same delivered in writing to the permittee.
  5. The permittee has failed to take positive actions to prohibit violations from recurring.
  6. The permittee has failed to make modifications within three days of receipt of the director's notice of same delivered in writing to the permittee.
  7. Pushcarts and other vestiges of the restaurant arcade vending zones may be removed by the department of public works, and a reasonable fee charged for labor, transportation, and storage, should the permittee fail to remove the items within 36 hours of receipt of the director's final notice to do so for any reason provided for under this article. If the action is taken based on subsection (7)a.2 or (7)a.3, the action shall become effective upon the receipt of such notice and the permittee shall have four hours to remove the items.
- b. Upon denial or revocation, the director shall give notice of such action to the applicant or the permittee in writing stating the action which has been taken and the reason thereof. If the action of the director is based on subsection (7)a.2 or (7)a.3, the action shall be effective upon giving such notice to permittee. Otherwise, such action shall become effective within ten days unless appealed to the city commission.
- (8) *Appeals.*
- a. Appeals shall be initiated within ten days of a permit denial or revocation by filing a written notice of appeal with the city manager, and a copy of same delivered the same day to the director. Any revocation effective immediately may also be appealed to the city commission by such filing within ten days.
  - b. The city manager shall place the appeal on the first non-planning and zoning city commission agenda for which reasonable notice can be given and shall notify the director of public works thereof. At the hearing upon appeal, the city commission shall hear and determine the appeal, and the decision of the city commission shall be final and effective immediately.
  - c. The filing of a notice of appeal by a permittee shall not stay an order by the director to remove a restaurant arcade vending zone or parts thereof. Vestiges of the restaurant arcade vending zone shall be removed immediately, as set out in subsection (7), pending disposition of the appeal and final decision of the city commission.
  - d. A permit which has been suspended or revoked pursuant to subsection (7)a.1, (7)a.2 or (7)a.4 may be reinstated by the director of the department of public works at such time as the permittee has demonstrated that the violation has been corrected to the satisfaction of the department of public works.
  - e. A new permit shall not be issued or an existing permit shall not be reinstated for a minimum period of six months after the issuance or reinstatement has been denied by the director of public works, or in the event of an appeal, by the city commission.
- (9) *Loudspeakers, etc.* Use of loudspeakers or recorded high volume music is not permitted.
- (10) *Obstruction of pedestrian path.* No portion of a pushcart, umbrella or canopy shall extend into the ten-foot pedestrian path.

- (11) *Merchandise vending.* No merchandise shall be vended or displayed other than that allowed for the area surrounding the restaurant arcade vending zone.
- (12) *Placement of vending pushcarts.* Vending pushcarts shall be placed between or parallel to the restaurant arcade's support columns, where applicable, and/or in the widened sidewalk area, if such exists.
- (13) *Hours, restrictions.* Pushcarts may be located in a restaurant arcade vending zone at any time of the day or night, unless the director determines that conditions warrant restricted hours.

(Ord. No. 10855, § 1, 3-14-91; Code 1980, § 39-17.3)

### **Sec. 39-37. - Limitations within Miami Arena special vending district.**

Vending within the Miami Arena special vending district shall be subject to all rules and regulations in this article, including [section 39-33](#), except as contrarily and specifically provided below:

- (1) No merchandise shall be vended or displayed other than food.
- (2) Pushcarts shall be located in their zones in a physical position commensurate with public works department sidewalk vending markings for the district.
- (3) No licensee shall operate, or hold a local business tax receipt for more than one pushcart in the herein district.
- (4) Vending zones.
  - a. Location of vending zones. Vending shall be prohibited in the Miami Arena special vending district except from a specifically approved location within the sidewalk areas generally designated on the graphics attached hereto as attachments A, B and C. [\[116\]](#) The selection of specific vending locations shall be the responsibility of the department of public works using the standards and criteria contained in this article. Vending zones and vendor locations may be deleted by the director of the department of public works upon a finding that the existence of such zone or location creates an obstruction to pedestrian or vehicular traffic, or otherwise creates a threat to the public health, safety, or general welfare. Additional locations may be approved by the director of the department of public works upon a finding that such vending locations are in a herein generally designated area, and otherwise satisfies all provisions of this article and other applicable regulations; however, vending shall not be permitted on sidewalks adjacent to or directly across from residential developments.
  - b. Limitations within vending zones.
    1. There shall be no more than one vendor permitted to operate from each vending location and such vendor may not move from location to location on the same day.
    2. Each vending location shall approximate the size of one permitted pushcart and shall be clearly marked on the sidewalk by the department of public works. The director shall keep an updated file showing and listing authorized locations, along with appropriate graphics, available for public and governmental agency perusal and use.
    3. All vending locations shall be spaced and oriented so as to maximize pedestrian flow and safety, and may exceed the linear frontage limitations of [section 39-33\(2\)e](#) herein.
- (5) All goods for sale, other than those on display on the pushcart, shall be stored within the structure of the pushcart.
- (6) It shall be unlawful for any vendor to use any noise-making device to solicit customers.
- (7) Vending pushcarts may not be chained or otherwise affixed to trees, light poles, sign

- stanchions or other stationary entities within the right-of-way.
- (8) Vending is prohibited within the herein vending district between the hours of 12:00 midnight to 10:00 a.m., and pushcarts shall not be located in this district during said hours. Further, vending shall not be permitted nor shall pushcarts be located within the district on event days except for a period of time beginning two hours immediately preceding, during and two hours following authorized event(s). For purposes of this section, events, event days and event times shall be as determined by the managing office of the Miami Arena and published by the management monthly in the Miami Arena Calendar of Events. Problems occasioned by changes in event times occurring subsequent to printing of said calendar, or errors therein, shall be ultimately resolved by the police department utilizing the most recent official records of the arena's management.
  - (9) Vending is prohibited, without exception, on any combination sidewalk and curb less than eight feet in width.
  - (10) Open flame cooking and use is prohibited, except as provided in sections [39-39](#) and [39-40](#)

(Code 1980, § 39-17.4; Ord. No. 12885, § 1, 2-8-07)

### **Sec. 39-37.1. - Limitations within Biscayne Boulevard special vending district.**

Vending within the Biscayne Boulevard special vending district ("district") shall be subject to all rules and regulations in this article, except as contrarily and specifically provided below:

- (1) No merchandise shall be vended or displayed other than:
  - a. Pre-packaged foods, as defined by 61C-1.001, Florida Administrative Code (2000), as amended, of the snack food type, in sealed bags.
  - b. Prepared foods including, but not limited to: ice cream, baked goods, fresh fruit and the like.
  - c. Unprepared foods including, but not limited to: hot dogs, crepes and the like. However, shiskabobs and like foods requiring heat generators, are prohibited.
  - d. Plants and flowers including, but not limited to: fresh cut or dried flowers or potted plants and the like.
- (2) Vending of merchandise shall also be in strict compliance with applicable regulations of the Florida Department of Agriculture, Florida Department of Business and Professional Regulation and Miami-Dade County.
- (3) Vending of merchandise shall be prohibited from any type of vehicle or stand other than a pushcart of the specific types and construction shown and described on composite "Exhibit B," attached to Ordinance No. 11212. Said pushcarts shall satisfy the above criteria and be inspected and certified initially and on an ongoing basis by the director and downtown NET administrator as having complied with this section. The director shall prepare a uniform pushcart certification form for usage in the district.
- (4) Pushcarts shall be located in their vending zones in a physical position commensurate with department of public works vending markings for the district.
- (5) No merchandise, supplies, containers or any other items related to the vendor shall be placed anywhere within the public right-of-way other than on or concealed within the pushcart, with the exception of one folding chair or wooden stool of a type approved by the director or Downtown Net Administrator, as compatible with the district's pushcart design requirements.
- (6) It shall be unlawful for any vendor to use any noise-making device to solicit customers.
- (7) Vending pushcarts may not be chained or otherwise affixed to trees, light poles, sign stanchions or other stationary entities on the sidewalk.
- (8) No licensee shall operate, or hold a local business tax receipt for more than one pushcart in the herein district.



- (9) Vending is prohibited within the district between the hours of 1:00 a.m. to 10:00 a.m., and pushcarts shall not be located in the district during said hours. Further, vending shall not be permitted nor shall pushcarts be located within the district on event days except for a period of time beginning two hours immediately preceding, during, and two hours following authorized event(s). For purposes of this section, events, event days and event times shall be as determined by the managing office of the New Arena and published in the New Arena's *Calendar of Events*, or a like official publication. Problems occasioned by changes in event times occurring subsequent to the publication of said calendar, or errors therein, shall be ultimately resolved by the police department or downtown NET office, utilizing the most recent official records of the New Arena's management.
- (10) Vending is permitted pursuant to the provisions of this article only on days when an event is scheduled in the New Arena.
- (11) Vending is prohibited, without exception, on any combination sidewalk and curb less than eight feet in width.
- (12) Open flame cooking and use is prohibited, except as provided in sections [39-39](#) and [39-40](#)
- (13) Vending zones.
  - a. Location of vending zones.
    1. Vending shall be prohibited in the district except from a specifically approved location within the sidewalk areas generally designated on the graphic attached to Ordinance No. 12002 as "Attachment A." However, the selection of specific vending zone locations subsequent to the establishment of this district shall be the responsibility of the director, using the standards and criteria contained in this article. Vending zones and vendor locations, including those initially established herein, may be deleted or relocated by the director upon a written finding that said action is necessary because the existing zone or location creates an obstruction to pedestrian or vehicular traffic, or otherwise creates a threat to the public health, safety or general welfare. Establishment of the alternate zone(s) or location(s) shall also require a written finding that such new vending location(s) is within the district and otherwise satisfies provisions of this article and other applicable regulations. However, vending shall not be permitted on sidewalks or rights-of-way adjacent to or directly across from residential developments.
    2. All vending locations, of which there shall be a maximum of eight, shall be spaced and oriented so as to maximize pedestrian flow and safety.
  - b. Limitations within vending zones.
    1. No more than one vendor shall be permitted to operate from each vending location, and said vendor may not move from location to location except as provided for in this section.
    2. Each vending location shall approximate the size of one permitted pushcart and shall be clearly identified by a metal (brass) pin and washer embedded in its proper location within the public right-of-way by the department of public works' survey division. The director shall keep an updated file showing and listing authorized locations, along with appropriate graphics, available for public and governmental agency perusal and use, and provide the downtown NET office and the city clerk with a certified copy of the current file.
  - c. Assignment of vendors to specific vending zones.
    1. Franchise rights. Vending zones within the district shall be occupied only by licensed vendors willing to pay the city for the opportunity and franchise right to vend, exclusively, from designated vending zones in the Biscayne Boulevard special vending district, subject to applicable rules, regulations, ordinances and

statutes governing vending. There shall be a franchise fee due of \$50.00 per month, for a total of \$600.00 per franchise period, for franchises. As a condition precedent to receiving a franchise, the total amount due for the franchise period shall be paid in full. Payment shall be by cashier's check, bank certified funds, or money order payable to the city. Failure to tender required payment on the date of the lottery shall invalidate such award and vacate the vending zone. All franchise fees shall be paid at the downtown NET office or its successor entity.

2. Lottery.

- i. The director shall establish and supervise a lottery system whereby those persons possessing a valid and appropriate local business tax receipt, appropriate state and local sales tax certificate(s), shall be chosen, by chance, for vending zones in this district. The director shall assign each vending zone a sequential number corresponding to a north to south and east to west rotation pattern of sequential locations on the vending map, which shall correspond to "Attachment A" of Ordinance No. 12002, as amended. All qualified vendors shall have their names placed into a container for a drawing by the director or NET administrator to determine which location shall serve as the initial vending zone for each vendor at the beginning of a franchise period. On the first day of each month following the first month of the franchise period, all vendors shall relocate, via rotation, to the next vending zone in the aforementioned sequence. All franchise rights shall transfer to the new location and cease in the prior location upon such rotation. Said rotation shall continue for the duration of the franchise period. At the conclusion of the franchise period all franchises shall be subject to a new lottery.
- ii. The director is authorized to issue a "Notice of Street Vending Franchise Opportunities" in the district. Said notice, for each franchise period, shall be publicly advertised in a newspaper of general circulation in approximately mid-August and mid-February of each calendar year, and shall indicate the pending availability of exclusive vending zones in the district and the terms of such availability, including the date, place and time of the lottery. Notices, as for a posted notice lottery, may also be given, but shall be considered courtesy notice only.
- iii. Utilizing the standards and criteria set forth in this article, the director may promulgate such reasonable supplementary rules, regulations and procedures as are necessary to implement and effectuate the herein lottery and vending zone assignment process.
- iv. For vending zones which may become available during the franchise period due to abandonment or director's action, the director shall specify the date, time and place for the holding of a special lottery for such designated vending zone(s), and shall publicly advertise said information as for a posted notice lottery.
- v. All franchise documents are nontransferable. Sale of a majority of stock in a corporate franchise by stockholders listed on the franchise application or sale of a majority interest in a partnership as listed on the franchise application shall be deemed a transfer of the franchise, which is prohibited. The franchise document shall be in the possession of the vendor at all times and shall be displayed to a police officer, code enforcement officer, downtown NET official or public works department representative upon request. Failure to immediately provide this document, along with a valid local business tax receipt, pushcart

- certification and sales tax certificate(s), shall be grounds for immediate removal of the pushcart from the vending zone and district, suspension of the franchise, and initiation of local business tax receipt and franchise revocation proceedings by the director or downtown NET administrator.
- vi. Franchises awarded pursuant to this section shall be subject to [section 39-29](#). Furthermore, the award of a franchise pursuant to this section does not grant or infer vested rights to the use of the public rights-of-way by the franchisee.
- vii. Any vending zone or franchise document issued pursuant to this section shall be subject to modification by ordinance at any time deemed necessary by the city commission. Vending in any vending zone may be temporarily suspended or relocated by the director upon reasonable notice when private or public construction or activities or health and safety concerns of the director make it unsafe or impractical to allow vending in that vending zone. Such suspension(s) which lasts for a continuous or cumulative period in excess of five days of a franchise period shall result in a pro rata refund of the lottery franchise fee paid by such suspended franchisee. No other payments or compensation shall be owed by the city or due the franchisee as a result of such suspension(s). A vendor so dispossessed, may, if possible, be offered a substitute-vending zone by the director without the necessity of lottery proceedings. Said substitute-location shall be valid for the balance of the time remaining on the vendor's franchise document for that vendor location, or until the substituted-for location is again available, whichever occurs first. If the vendor accepts a substitute-location, the refund shall be only for the actual days of suspended operation, and shall not include the day(s) of operation in the substitute location.
- viii. Vending activity suspended pursuant to sections [39-29](#) and [39-38](#), or revoked due to unauthorized absence or violations of the codes of the city, county or general law, shall not be the basis for any pro rata refund of a franchise fee. Revocation of franchise documents based on unauthorized absences or violations shall result in a forfeiture of the entire franchise fee.
- d. All participants in lottery proceedings pursuant to this section shall submit, as a condition precedent to participating, a copy of an appropriate valid local business tax receipt, certification, pursuant to section 39-7.1(3), that the pushcart which will be used in this district has been approved, and sales tax certification.
- e. Unauthorized absence from a designated vending zone shall constitute a basis for suspension and revocation of a franchise document. Upon certification by the director or downtown NET administrator that a vending zone has been unoccupied for a continuous period of ten event days, for reasons other than those mentioned in subsection (13)c.2.vii or [section 39-29](#), the director or downtown NET administrator shall notify the vendor of the intent to revoke the vendor's franchise unless clear evidence of proof of the vendor's activity during the ten event-day period in question is provided to the director. Subsequent to ten-day notice mailed by certified mail to the address shown on the vendor's lottery application form, the director shall conduct a hearing, and may revoke the vending franchise and reward the franchise to a different vendor, pursuant to a posted notice lottery, for the balance of that franchise period. The vendor subject to such revocation may appeal the director's decision in the same manner provided in [section 54-230](#)
- f. Any franchise incurring three written notices of violation of this article shall be the

subject of the following franchise revocation proceedings:

1. When violations occur, the franchisee shall be notified by the director or downtown NET office in person or via certified mail. The first violation notice or citation shall be a reprimand; the second violation notice or citation shall be a warning; the third violation notice or citation shall result in an automatic revocation of franchise document, immediate removal of the franchisee's pushcart from the district, and banishment of the violator from the district for a period of one calendar year.
  2. Revocations may be appealed in the same manner provided in [section 54-230](#). An appeal shall not stay an order by the director or NET office to remove a pushcart from the district.
- g. Fees collected under this subsection are declared to be franchise fees charged for the right to exclusive commercial use of a portion of the public rights-of-way in the New Arena downtown area, and are in addition to local business taxes imposed by law and other permit fees which may be collected to defray the cost of administration of this subsection. All franchise fees collected by the director of finance or his designee pursuant to this section shall be placed in a special account established for the "Biscayne Boulevard Special Vending District," and shall be used to defray the cost of administering and regulating the district's vendors.
- h. The director shall design and distribute to those awarded a vending zone a franchise document identifying the person or entity chosen by lottery, the specific location where said person or entity is to be allowed to initially vend exclusively during the vending period, and the duration of such entitlement.
- i. All franchise documents issued for vending activity in this district shall only be valid during one franchise period, and shall expire on the expiration date shown on the franchise document and records of the director. Upon such expiration the vendor's exclusive right to such vending zone shall terminate, and vending rotation rights shall once again be awarded pursuant to the lottery procedures of this section.
- j. Liability and insurance.
1. Prior to the issuance of a franchise document, the vendor shall furnish the director with a signed statement that said vendor shall hold harmless the city, its officers and employees, and shall indemnify the city, its officers and employees for any claims for damages to property or injury to persons which may be occasioned by any activity carried on under the terms of the franchise document and associated local business tax receipt.
  2. Prior to the issuance of a franchise document, said vendor shall also furnish and maintain such public liability and property damage from all claims and damage to property or bodily injury, including death, which may arise from operations under the franchise document and associated local business tax receipt or in connection therewith. Such insurance shall provide coverage of not less than \$500,000.00 for bodily injury, and property damage respectively per occurrence. Such insurance shall be without prejudice to coverage otherwise existing therein and shall name as additional insured the city, its officers and employees, and shall further provide that the policy shall not terminate or be canceled prior to the completion of the franchise period without 45 days' written notices to the risk management division and the director at the addresses shown in the franchise document.
- k. Sales tax certification. Prior to the issuance of franchise documents, said vendor shall also furnish original evidence of a valid certificate of resale or equivalent document from the Florida Department of Revenue and Miami-Dade County, if applicable, evidencing that said vendor and the specific vending activity authorized by said

franchise document have been permitted by said tax collection entities to the extent mandated by law. Franchisee(s) shall furnish, upon demand, evidence that the herein requested certificate of resale or equivalent document is current. Failure to maintain said certification shall constitute a basis for suspension and/or revocation of a franchise document.

1. State license inspection and certification. Prior to issuance of a franchise document, the vendor shall also furnish original evidence of a valid license issued, upon inspection, by the state department of business and professional regulation (for vending prepared food, as defined by state regulations) and/or the state department of agriculture (for vending prepackaged food, as defined by state regulations).

(Ord. No. 12002, § 2, 12-14-00; Ord. No. 12885, § 1, 2-8-07)

### **Sec. 39-38. - Prohibited conduct.**

No vendor shall:

- (1) Leave any stand or motor vehicle unattended.
- (2) Store, park, or leave any stand overnight on any street or sidewalk, or park any motor vehicle other than in a lawful parking space, in conformance with city and state parking regulations.
- (3) Sell food for immediate consumption unless he has available for public use his own litter receptacle, which is available for his patrons' use.
- (4) Allow or keep any animals in motor vehicles or stands.
- (5) Leave any location or vending zone without first picking up, removing, and disposing of all trash and refuse remaining within a 15-foot radius. Each vendor shall be responsible for maintaining a 15-foot radius trash and refuse clear area around himself. Said area shall overlap other vendor cleanup areas and no vendor shall leave a location, or vending zone, without cleaning up as required.
- (6) Allow any items relating to the operating of the vending business to be placed anywhere other than in, on, or under the stand or motor vehicle.
- (7) Set up, maintain, or permit the use of any table, crate, carton, rack, or any other device to increase the selling or displaying capacity of his stand, or motor vehicle, where such items have not been described in his/her application.
- (8) Solicit or conduct business with persons in motor vehicles located on traffic lanes of public streets and highways.
- (9) Sell anything other than that for which he is licensed to vend.
- (10) Use any noise-making device after 9:00 p.m., except during special events, and at no time shall such a vendor use his traffic warning device on any vehicle, except to give necessary signals while in traffic. It shall be unlawful for any vendor to use any noise-making device that either annoys, disturbs, injures, or endangers the comfort, repose, health, peace, or safety of others within the city. Any vendor who violates this section shall upon written notice from the city manager or his authorized representative remove said noise-making device from the vehicle or reduce the volume of such noise-making device so that the same shall not be in violation of this section. Failure to comply with such notice shall subject such a vendor to the penalties as set forth in [section 39-50](#)
- (11) Allow the stand or any other item relating to the operation of the vending business to lean against or hang from any building or other structure lawfully placed on public property.
- (12) Allow any animals to remain within 25 feet of a stand for a period longer than necessary to complete a sale to the person having possession, or control of said animals.
- (13) No vendor vending from a motor vehicle shall:

- a. Conduct his/her business in such a way as would restrict or interfere with the ingress or egress of the abutting property owner or tenant, or create or become a public nuisance, increase traffic congestion or delay, or constitute a hazard to traffic, life or property, or an obstruction to adequate access to fire, police or sanitation vehicles.
- b. Stop, stand, or park his motor vehicle upon any street, or permit it to remain there except on the roadway at the curb for the purposes of vending therefrom or in instances where there is no curb, off the roadway. In either instance, sales shall be to occupants of abutting property only.
- c. Stop, stand, or park his motor vehicle upon any street for the purpose of selling, or sell on any street under any circumstances during the hours when parking, stopping or standing has been prohibited by signs or curb markings or is prohibited by statute or ordinance.
- d. Remain in any one place for a period longer than necessary to make a sale after having been approached or stopped for that purpose.
- e. Stop, stand, or park his motor vehicle within 20 feet of any intersection, except that vehicles vending products likely to attract children as customers shall park curbside when stopping to make a sale, as close as possible to a pedestrian crosswalk without entering the intersection or otherwise interfering with the flow of traffic.
- f. Vend within a restricted or special vending district.
- g. Vend anywhere prohibited by [section 39-33](#)(2) through (8).

(Ord. No. 9880, § 1, 9-13-84; Ord. No. 10045, § 1, 9-26-85; Ord. No. 10499, § 1, 10-27-88; Code 1980, § 39-18)

**City Code cross references**—Parking for purpose of selling merchandise from vehicle generally prohibited, [§ 35-10](#)(a)(4); towing of vehicles, [§ 42-101](#) et seq.

### **Sec. 39-39. - Open flame cooking.**

Open flame cooking is prohibited; except that such activity may take place as an integral part of a public assembly as permitted by the fire-rescue department, or in conjunction with the street festival, as approved by city commission resolution. The permitted public assembly or street festival exception shall be subject to the festival organizers obtaining permits from the fire-rescue department and such other departments or agencies as may be required by law.

(Ord. No. 10869, § 2, 4-11-91; Ord. No. 10891, § 1, 6-20-91; Code 1980, § 39-18.1)

### **Sec. 39-40. - Open flame use.**

Open flame use is prohibited; except that such activity may take place as an integral part of a public assembly as permitted by the fire-rescue department, or in conjunction with a street festival, as approved by city commission resolution. The permitted public assembly or street festival exception shall be subject to the festival organizers obtaining permits from the fire-rescue department and such other departments or agencies as may be required by law.

(Ord. No. 10891, § 1, 6-20-91; Code 1980, § 39-18.2)

### **Sec. 39-41. - Size requirements for vending stands.**

No stand shall exceed 3½ feet in width and six feet in length and five feet in height exclusive of the height of umbrellas, canopies, and similar devices. Canopies and umbrellas shall have a minimum seven-foot clearance above ground level.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-19)

**Sec. 39-42. - Health and sanitation requirements for food vending.** 

Vendors of food shall comply with the requirements and standards of the department of health and the following:

- (1) The equipment used in vending food shall be inspected by department of health upon application for a license and receive a certificate of inspection upon compliance with this section.
- (2) Each food vending business shall be so inspected at least twice a year.

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-20)*

**Sec. 39-43. - Safety requirements.** 

All motor vehicles in or from which food is prepared or sold shall comply with the following requirements:

- (1) All equipment installed in any part of the vehicle shall be secured in order to prevent movement during transit and to prevent detachment in the event of a collision or overturn.
- (2) All utensils shall be stored in order to prevent their being hurled about in the event of a sudden stop, collision or overturn. A safety knife holder shall be provided to avoid loose storage of knives. Any glass must be safety plate clearly identified by its manufacturer as such.
- (3) Compressors, auxiliary engines, generators, batteries, battery chargers, gas-fueled water heaters, and similar equipment shall be installed so as to be accessible only from outside the vehicle.
- (4) All heated stands shall have an easily accessible fire extinguisher with a valid inspection sticker.

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-21)*

**Sec. 39-44. - Advertising.** 

No advertising, except the posting of prices, shall be permitted on or attached to any stand or motor vehicle, except to identify the name of the product. This section does not prohibit the use of umbrellas bearing logos of products sold at the stand or motor vehicle to which it is attached.

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-22)*

**Sec. 39-45. - Renewal.** 

Subject to the provisions of [section 39-29](#), all licenses are valid for the entire licensing period unless revoked or suspended prior to expiration. Application to renew a BTR shall be made not later than 30 days before the expiration of the current BTR in accordance.

*(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-23; Ord. No. 13105, § 2, 10-8-09)*

**Sec. 39-46. - Denial, suspension, revocation.** 

Any license or permit may be denied, suspended or revoked in accordance with the procedures contained in [chapter 31](#) for any of the causes set forth in said [chapter 31](#) in addition to the following causes:

- (1) Fraud or misrepresentation contained in the application for the BTR or permit.
- (2) Fraud or misrepresentation made in the course of carrying on the business of vending.

- (3) Carrying or possessing dangerous weapon.
- (4) Conduct of the BTR holder permitted business in such manner as to create a public nuisance, or constitute a danger to the public health, safety, welfare or morals.
- (5) Conduct which is contrary to the provisions of this article.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-24; Ord. No. 13105, § 2, 10-8-09)

### **Sec. 39-47. - Notice on premises that uninvited vendors, solicitors, peddlers, etc., are not wanted.**

- (a) It shall be the duty of the person in possession of any premises who desires that the occupants of the premises remain unmolested by the visits of uninvited solicitors, peddlers, vendors, itinerant merchants, door-to-door canvassers or hawkers to post in a conspicuous place near the door or on the premises a sign in letters at least 1½ inches high with the words "no peddlers," "no solicitors," "no trespassing" or otherwise signifying externally the wish for the occupants of the premises to remain unmolested by such visitors.
- (b) It shall be unlawful for any uninvited solicitors, peddlers, vendors, itinerant merchants, door-to-door canvassers or hawkers to visit or go upon any premises which have been posted with a notice as prescribed in this section, to the effect that the person in possession or the occupants of the premises desire to remain unmolested.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-25)

### **Sec. 39-48. - Exemptions as to farm products.**

- (a) Nothing contained in sections [39-28](#) or [39-32](#)(3) shall be construed to affect or apply to the producer of farm or grove products where the same are being offered for sale or sold by the farmer or grower producing such products.
- (b) The farmer or grower offering for sale or selling in the city the farm or grove products produced by such farmer or grower shall furnish satisfactory evidence that such products being sold or offered for sale have been grown by him.
- (c) The members of the police department, as well as the license inspectors, are authorized and directed to obtain affidavits or written statements from such grower or producer of the farm or grove products when the same are being offered for sale or sold by him in the city, such affidavit or written statement showing and stating that the farm or grove products have been grown by such farmer or grower.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-26)

### **Sec. 39-49. - Exemptions for vendors who exclusively vend written matter.**

Vendors who exclusively vend written matter are exempt from the following provisions of this article: sections [39-28](#) through [39-33](#), [39-38](#)(1) and (2), [39-38](#)(11), and [39-41](#).

(Ord. No. 10045, § 1, 9-26-85; Code 1980, § 39-26.1)

### **Sec. 39-50. - Penalty.**

Except as may be provided in [section 39-51](#), any person violating any provision of this article shall be guilty of a misdemeanor and upon conviction, shall be punished as provided in [section 1-13](#).

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-27)

### **Sec. 39-51. - Violation a nuisance; summary abatement.**



The placement of any stand or device on any sidewalk or street in violation of the provisions of this article is declared to be a public nuisance. The police department may cause the removal of any stand or device found on a sidewalk or street in violation of this article and is authorized to store such stand or device until the owner thereof shall redeem it by paying the removal and storage charges therefor to be established by the police department.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-27.1)

### Sec. 39-52. - Enforcement of article.

It shall be the duty of the members of the police department, BTR inspectors, and code inspectors of the city, to enforce the terms and conditions of this article, and if any person is found violating the provisions of this article to arrest such person and hold such violator for proper legal action in the county court or cite such person for appearance before, and action by, the city's code enforcement board.

(Ord. No. 9880, § 1, 9-13-84; Code 1980, § 39-27.2; Ord. No. 13105, § 2, 10-8-09)

---

#### FOOTNOTE(S):

---

<sup>(115)</sup> *County Code cross reference—Similar provisions, § 21-27.1. [\(Back\)](#)*

<sup>(116)</sup> **Editor's note**— *Attachments A, B and C to Ord. No. 10891, adopted June 20, 1991, from which this section is derived, are not set out, but are on file and available for public inspection in the office of the city clerk. [\(Back\)](#)*

**EXHIBIT Y**

Print

## Municipal Code of Chicago

### **4-244-010 Definitions.**

As used in this chapter:

“Commissioner” means the commissioner of business affairs and consumer protection or the commissioner's designee.

“Department” means the department of business affairs and consumer protection.

“Licensee” means any person holding or required to hold a license under this Chapter 4-244.

“Millennium Park” has the meaning ascribed to the term in Section 10-36-140.

“Peddler” or “street peddler” means any individual who, going from place to place, whether on private property or on the public way, sells, offers for sale, sells and delivers, barter or exchanges any goods, wares, merchandise, wood, fruits, vegetables or produce from a vehicle or otherwise. The term “peddler” does not include (1) a “grower” or “producer” as defined in Section 4-12-010 of this Code, or (2) any class of peddler specifically defined and licensed or required to be licensed under other chapters of this Code, including, but not limited to, (i) any junk peddler within the meaning of Section 4-6-150; (ii) any merchant within the meaning of Chapter 4-212 of this Code, or (iii) any mobile food dispenser within the meaning of Chapter 4-8 of this Code.

“Perform” means and includes, but is not limited to, the following activities: acting, singing, playing musical instruments, pantomime, juggling, magic, dancing or reciting.

“Performer” means any person holding or required to hold a street performer permit under this chapter.

“Public area” means any sidewalk, parkway, playground or other public way located within the corporate limits of the City. The term “public area” does not include transit platforms and stations operated by the Chicago Transit Authority or the Metropolitan Transportation Authority.

“Special event” means any special event conducted by the City of Chicago, including, but not limited to, events conducted with the permission of the Chicago Park District in parks or other facilities operated by the Chicago Park District. (Prior code § 160-1; Amend Coun. J. 10-7-09, p. 72718, § 3; Amend Coun. 5-9-12, p. 27485, § 117)

### **4-244-030 License – Required.**

(a) It shall be unlawful for any person to engage in the business of a peddler without first having obtained a street peddler a license under this chapter.

(b) Any person violating this section shall be fined not less than \$50.00 nor more than \$200.00 for each offense. Each day such violation continues shall constitute a separate and distinct offense.

(Added Coun. J. 12-9-92, p. 25465; Amend Coun. 5-9-12, p. 27485, § 119)

#### **Disclaimer:**

This Code of Ordinances and/or any other documents that appear on this site may not reflect the most current legislation adopted by the Municipality. American Legal Publishing Corporation provides these documents for informational purposes only. These documents should not be relied upon as the definitive authority for local legislation. Additionally, the formatting and pagination of the posted documents varies from the formatting and pagination of the official copy. The official printed copy of a Code of Ordinances should be consulted prior to any action being taken.

For further information regarding the official version of any of this Code of Ordinances or other documents posted on this site, please contact the Municipality directly or contact American Legal Publishing toll-free at 800-445-5588.

© 2011 American Legal Publishing Corporation  
[techsupport@amlegal.com](mailto:techsupport@amlegal.com)  
1.800.445.5588.

Print

## Municipal Code of Chicago

### **4-244-030 License – Required.**

(a) It shall be unlawful for any person to engage in the business of a peddler without first having obtained a street peddler a license under this chapter.

(b) Any person violating this section shall be fined not less than \$50.00 nor more than \$200.00 for each offense. Each day such violation continues shall constitute a separate and distinct offense.

(Added Coun. J. 12-9-92, p. 25465; Amend Coun. 5-9-12, p. 27485, § 119)

**Disclaimer:**

This Code of Ordinances and/or any other documents that appear on this site may not reflect the most current legislation adopted by the Municipality. American Legal Publishing Corporation provides these documents for informational purposes only. These documents should not be relied upon as the definitive authority for local legislation. Additionally, the formatting and pagination of the posted documents varies from the formatting and pagination of the official copy. The official printed copy of a Code of Ordinances should be consulted prior to any action being taken.

For further information regarding the official version of any of this Code of Ordinances or other documents posted on this site, please contact the Municipality directly or contact American Legal Publishing toll-free at 800-445-5588.

© 2011 American Legal Publishing Corporation  
[techsupport@amlegal.com](mailto:techsupport@amlegal.com)  
1.800.445.5588.

**EXHIBIT Z**

## Lindsey Frank

---

**From:** kdeeley@fec.gov  
**Sent:** Wednesday, October 31, 2012 5:35 PM  
**To:** lindsey.frank74@gmail.com; Lindsey Frank  
**Cc:** rknop@fec.gov  
**Subject:** Fw: SWP: request for an extension

Mr. Frank:

The Commission has granted your request for an extension of time until November 8, 2012. Please let us know if you have any questions.

Regards,  
Kevin

Kevin Deeley  
Federal Election Commission  
999 E Street NW  
Washington, DC 20463  
(202) 694-1556 | kdeeley@fec.gov