

EXHIBIT A

Record Description	Bates Number	Disposition	Description of Applicable Exemptions
Production 1			
Information Issue Paper (Oct. 6, 2016)	USCBP000001-04	Released with redactions	<p>Reprocessed with fewer redactions: 000003</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Descriptions of analyses being conducted by CBP personnel to evaluate the feasibility and effectiveness of using social media information in CBP’s law enforcement and border security mission in order to inform future policy decisions by CBP decision makers. • Descriptions of the content and status of a draft, pre-decisional report on the use of social media in CBP operations being prepared to inform future policy decisions by CBP decision makers. • Descriptions of the subject of ongoing policy deliberations and recommendations for future activities relating to the operational use of social media. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that</p>

			<p>would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP’s operational use of social media • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of the law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of vulnerabilities and limitations in CBP’s operational use of social media.
<p>CBP Use of Social Media Paper (May 25, 2016)</p>	<p>USCBP000005-07</p>	<p>Released with redactions</p>	<p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information,</p>

			<p>would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Information that could reveal details about a specific law enforcement investigation, including information that could identify the subject of a law enforcement investigation and the specific techniques used to uncover potentially illicit activity in an ongoing investigation. • Descriptions of vulnerabilities and limitations in CBP’s operational use of social media.
<p>CBP Use of Social Media Paper (Sept. 26, 2016)</p>	<p>USCBP000008-12</p>	<p>Released with redactions</p>	<p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p>

			<ul style="list-style-type: none"> • Descriptions of analyses being conducted by CBP personnel to evaluate the feasibility and effectiveness of using social media information in CBP’s law enforcement and border security mission in order to inform future policy decisions by CBP decision makers. • Descriptions of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Descriptions of specific law enforcement techniques and types of analysis that CBP does
--	--	--	--

			or does not utilize when using publicly available social media information.
Social Media Briefing Paper	USCBP000013-15	Released with redactions	<p>Reprocessed with fewer redactions: 00014</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. • Information prepared by CBP personnel to inform CBP decision makers of the status and scope of internal CBP deliberations regarding a proposal to modify certain forms and applications used to obtain immigration and travel benefits. • Descriptions of the status and scope of inter-agency consultations and deliberations regarding proposed modifications to certain forms and applications used to obtain immigration and travel benefits. • Description of the status and contents of a predecisional draft report regarding privacy requirements and the non-final

			<p>recommendations and assessments of the report's authors.</p> <ul style="list-style-type: none"> • Recommended responses to hypothetical questions contained in briefing materials developed by CBP staff to suggest responses for agency decision makers if asked in future inquiries about CBP's operational use of social media. <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information in law enforcement operations. • Information regarding vulnerabilities and limitations in CBP's operational use of social media. • Descriptions of the scope and investigatory focus of CBP's operational use of social media.
Information Issue Paper (June 2, 2016)	USCBP000016-17	Released with redactions	Reprocessed with fewer redactions: 000017

			<p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of proposed future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. • Description of the scope and subject matter of assessment being conducted by CBP to inform agency deliberations and develop recommendations for CBP policy makers regarding the future use of social media in CBP’s border security mission. • Description of the status and contents of a draft report regarding proposed areas of investigative focus and future developments, prepared to inform agency deliberations and make recommendations to CBP decision makers regarding the operational use of social media within CBP. <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for</p>
--	--	--	--

			<p>law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information in law enforcement operations.
Information Issue Paper (Aug. 30, 2016)	USCBP000018-19	Released with redactions	<p>Reprocessed with fewer redactions: 000019</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency's decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations.

			<ul style="list-style-type: none"> • Description of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. • Descriptions of the content and status of a draft, pre-decisional report on the use of social media in CBP operations being prepared to inform future policy decisions by CBP decision makers. • Description of the scope and subject matter of assessment being conducted by CBP to inform agency deliberations and develop recommendations for CBP policy makers regarding the future use of social media in CBP's border security mission. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for</p>
--	--	--	--

			<p>law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information in law enforcement operations.
Information Issue Paper (Apr. 20, 2017)	USCBP000020-22	Released with redactions	<p>Reprocessed with fewer redactions: 0000020, 000022</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency memorandum that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency's decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. • Description of recommended future uses and techniques for social media information being

			<p>evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations.</p> <ul style="list-style-type: none"> • Descriptions of the content and status of a draft, pre-decisional report on the use of social media in CBP operations being prepared to inform future policy decisions by CBP decision makers. • Description of the scope and subject matter of assessment being conducted by CBP to inform agency deliberations and develop recommendations for CBP policy makers regarding the future use of social media in CBP's border security mission <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement</p>
--	--	--	---

			<p>techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of vulnerabilities and limitations in CBP's operational use of social media.
Privacy Threshold Analysis: Electronic Visa Update System (EVUS)	USCBP000023-39	Released with redactions	<p>Reprocessed with fewer redactions: 000024, 00025, 00037; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency's decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of privacy risk mitigation strategies and assessments being proposed by CBP to DHS Privacy in connection with potential changes to the use of social media in CBP's law enforcement and border security mission.

			<ul style="list-style-type: none"> • Descriptions of the status and scope of inter-agency consultations and deliberations regarding proposed record retention plan. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Information regarding the factors considered and criteria utilized when determining whether to use social media information in conducting CBP's law enforcement and border security
--	--	--	--

			<p>mission, including the vetting of international travelers or applicants for immigration benefits.</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the law enforcement processes utilized and information consulted when vetting international travelers or applicants for immigration benefits.
<p>DHS Operational Use of Social Media, Office of Internal Affairs: Use of Social Media for Criminal Investigations</p>	<p>USCBP000040-47</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000041, 000043, 000047</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes a description of the content and status of a draft, pre-decisional report on the use of social media in CBP operations prepared to inform future policy decisions by CBP leadership regarding the use of social media by CBP.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly</p>

			<p>unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Information relating to unique types of evidence obtained using the law enforcement techniques at issue.
Privacy Threshold Analysis: Pilot Evaluation	USCBP000048-57	Released with redactions	<p>Reprocessed with fewer redactions: 000050, 000052, 000053, 00056; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include the name of company providing unique, proprietary services to CBP.</p>

			<p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Description of the scope and subject matter of assessment being conducted by CBP to inform agency deliberations and develop recommendations for CBP policy makers regarding the future use of social media in CBP’s border security mission. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Description of the content and status of a draft, pre-decisional assessment on the use of social media in CBP operations. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p>
--	--	--	--

			<p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Information relating to unique types of evidence obtained using the law enforcement techniques at issue.
Production 2			
Talking Points: October 2016 Electronic System for Travel Authorization Enhancements	USCBP000058-60	Released with without redactions	N/A

<p>Privacy Threshold Analysis: IntelCenter Social Media Database Ingestion into ATS</p>	<p>USCBP000061-70</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000062, 000068; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include:</p> <ul style="list-style-type: none"> • Sensitive information about software and database, including capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software. • Information that the database contains <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Descriptions of recommended future uses and techniques for social media information being evaluated and considered by CBP personnel pending a decision on the feasibility and effectiveness of incorporating such uses and techniques into CBP operations. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP
---	-----------------------	---------------------------------	--

			<p>activity relating to social media, and descriptions of the proposed activity that is pending approval.</p> <ul style="list-style-type: none"> • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, operational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of specific types of information CBP intends to access, and how it intends to
--	--	--	---

			<p>utilize such information in conducting particular law enforcement functions.</p> <ul style="list-style-type: none"> • Detailed descriptions of how CBP intends to record, report, and store law enforcement information gathered • Descriptions of the scope and investigatory focus of CBP's operational use of social media
Privacy Threshold Analysis: Office of Intelligence and the Office of Professional Responsibility	USCBP000071-80	Released with redactions	<p>Reprocessed with fewer redactions: 00072, 00078; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency's decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly</p>

			<p>unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue • Descriptions of the scope and investigatory focus of CBP's operational use of social media • Information that could reveal details about a specific law enforcement investigation, including information that could identify the subject of such investigation and the specific techniques used to uncover potentially illicit activity in an ongoing investigation. • Information regarding the factors considered and criteria utilized when information is reported to the Joint Intake Center • Descriptions of criteria for utilizing particular law enforcement techniques, which could reveal
--	--	--	---

			the degree to which such techniques are available.
Privacy Threshold Analysis: Youtube Access for CBP	USCBP000081-87	Released with redactions	<p>Reprocessed with fewer redactions: 00082, 00086; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p>

<p>DHS Operational Use of Social Media: Office of Trade: Forced Labor Division</p>	<p>USCBP000088-96</p>	<p>Released with redactions</p>	<p>Reprocessed without redactions: Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) - Exemption (b)(5) has been applied to attorney/client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing consultations with CBP Office of Chief Counsel.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p>
--	-----------------------	---------------------------------	--

			<ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media.
DHS Operational Use of Social Media: Office of Professional Responsibility: Use of Social Media for Administrative Investigations	USCBP000097-105	Released with redactions	<p>Reprocessed with fewer redactions: 00098; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) - Exemption (b)(5) has been applied attorney-client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing consultations with CBP Office of Chief Counsel.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for</p>

			<p>law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Detailed descriptions of how CBP intends to record, report, and store law enforcement information gathered
DHS Operational Use of Social Media: Office of Professional Responsibility: Use of Social Media for Criminal Investigations	USCBP000106-15	Released with Redactions	<p>Reprocessed with fewer redactions: 000107; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>(b)(5) - Exemption (b)(5) has been attorney/client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing consultations with CBP Office of Chief Counsel.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p>

			<p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Detailed descriptions of how CBP intends to record, report, and store law enforcement information gathered •
DHS Operational Use of Social Media: Office of Professional Responsibility: Use of Social Media for Background Investigations and Periodic Reinvestigations	USCBP000116-24	Released with redactions	<p>Reprocessed with fewer redactions: 000117, 000121, 000122, 000124; Header Information (Phone Numbers and Email Addresses for DHS Privacy Office)</p> <p>Exemption (b)(5) has been applied to attorney-client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing the subject matter of consultations with the CBP Office of Chief Counsel for the purpose of providing legal advice.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record,</p>

			<p>which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Detailed descriptions of how CBP intends to record, report, and store law enforcement information gathered •
Production 3			
CBP Directive, January 2, 2015	USCBP000125-36	Released with redactions	<p>Reprocessed with fewer redactions: 000136</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement</p>

			<p>purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. Descriptions of criteria for utilizing particular law enforcement techniques, which could reveal the degree to which certain such techniques are available.
Interim Standard Operating Procedure	USCBP000137-41	Released with redactions	<p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names of non-SES DHS employees and signatures of DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing</p>

			<p>alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Information that would enable access to and/or manipulation of law enforcement processes, databases, and/or information, including email addresses and methods used internally by CBP personnel in the approval process for engaging in the operational use of social media. • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
<p>Internal Memorandum, February 15, 2018</p>	<p>USBP000142-46</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000142</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement</p>

			<p>techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Descriptions of criteria for utilizing particular law enforcement techniques, which could reveal the degree to which such techniques are available. Information that would enable access to and/or manipulation of law enforcement processes, databases, and/or information, including email addresses, network addresses, URLs and methods used internally by CBP personnel in the approval process for engaging in the operational use of social media.
Email re DHS/CBP Privacy Assessment, March 27, 2019	USCBP000147-48	Released with redactions	<p>Reprocessed with fewer redactions: 000147,, 000148</p> <p>(b)(6) - Exemptions (b)(6) has been applied to information contained in the record that identifies a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of individuals appearing in records relating to the operational use of social media.</p> <p>(b)(7)(C) – Exemption (b)(7)(C) has been applied to information contained in the record which was compiled for law enforcement purposes, that identifies a particular individual, and disclosure would constitute a clearly</p>

			unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees appearing in records compiled for law enforcement purposes relating to the operational use of social media.
Privacy Threshold Analysis: Office of Intelligence and the Office of Professional Responsibility, July 2, 2018	USCBP000149-60	Released with redactions	<p>Reprocessed with fewer redactions: 000150, 000158</p> <p>(b)(5) - Exemption (b)(5) has been applied to portions of this intra-agency document that would be normally privileged in the civil discovery context. Specifically, exemption (b)(5) has been applied to the following:</p> <ul style="list-style-type: none"> • Attorney-client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing the subject matter and content of communications between the CBP Office of Chief Counsel and CBP personnel conducted for the purpose of providing legal advice. • Deliberative process privileged information. The deliberative process privilege applies to information that is predecisional and deliberative and withholding the information is necessary to protect the agency's decision-making processes. Redacted information includes descriptions of the status and scope of predecisional deliberations regarding the development of training for conducting social media activities, and recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed

			<p>CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. Opinions and recommendations from DHS Privacy to CBP regarding future steps to evaluate and achieve compliance with privacy laws and policy.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of the specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media.
--	--	--	--

			<ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of specific types of information CBP intends to access, and how it intends to utilize such information in conducting particular law enforcement functions.
<p>DHS Operational Use of Social Media: Office of Intelligence and Investigative Liaison</p>	<p>USCBP000161-69</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redaction: 000163</p> <p>(b)(5) – Exemption (b)(5) has been applied to attorney-client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing consultations with CBP Office of Chief Counsel.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and</p>

			<p>procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of specific types of information CBP intends to access, and how it intends to utilize such information in conducting particular law enforcement functions.
DHS Operational Use of Social Media: Office of Intelligence and Investigative Liaison	USCBP000170-77	Released with redactions	<p>Reprocessed with fewer redactions: 000171 (b)(5) - Exemption (b)(5) has been applied to portions of this intra-agency document that would be normally privileged in the civil discovery context. Specifically, exemption (b)(5) has been applied to the attorney-client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The</p>

			<p>exemption was applied to information describing the subject matter and content of communications between the CBP Office of Chief Counsel and CBP personnel conducted for the purpose of providing legal advice.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names and phone numbers of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and
--	--	--	---

			<p>third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue.</p> <ul style="list-style-type: none"> • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
DHS Operational Use of Social Media: U.S. Border Patrol, November 27, 2017	USCBP000178-91	Released with redactions	<p>Reprocessed with fewer redactions: 000179, 000190; Header Information (Email Phone Numbers and Email Addresses of DHS Privacy Office)</p> <p>(b)(5) - Exemption (b)(5) has been applied to attorney/client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to information describing the subject matter and content of communications between the CBP Office of Chief Counsel and CBP personnel conducted for the purpose of providing legal advice.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p>

			<p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP's operational use of social media.] • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
CBP Operational Use of Social Media, Rules of Behavior	USCBP000192-96	Released with redactions	Reprocessed with fewer redactions: 000196; Header Information (Phone Numbers and Email Addresses of DHS Privacy Office)

			<p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Information regarding the investigatory focus of certain law enforcement activities regarding unauthorized access to government information and suspected techniques, tactics, and/or procedures of illicit actors that may access classified or otherwise protected information. • Information that would enable access to internal processes used by CBP to manage and secure information technology systems used in support of CBP's law enforcement functions.
Production 4			
Contract Number HSHQDC-12-D-00013, Order Number 70B04C18F00001093	USCBP000197-212	Released with redactions	<p>Reprocessed with fewer redactions: 000198, 000199, 000206, 000207</p> <p>(b)(3)(A) – Exemption (b)(3)(A) has been applied to records or information that are exempted from disclosure by statute. Redactions applied to this information include tax information withheld pursuant</p>

			<p>to 26 U.S.C. § 6103, which prohibits the disclosure of tax returns or return information.</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include unit prices and ext. prices, where the disclosure of such information would reveal nonpublic commercial information furnished by the contractor or may be used to reverse engineer the contractor's proprietary technical approach under a government contract.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, signatures, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement</p>
--	--	--	--

			<p>techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Information, such as the quantity and period of performance, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.
<p>Award Contract Number HSHQDC13D00027, Order Number 70B04C18F00001257</p>	<p>USCBP000213-34</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000215, 000216, 000234</p> <p>(b)(3)(A) – Exemption (b)(3)(A) has been applied to records or information that are exempted from disclosure by statute. Redactions applied to this information include tax information withheld pursuant to 26 U.S.C. § 6103, which prohibits the disclosure of tax returns or return information.</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include unit prices and ext. prices, where</p>

			<p>the disclosure of such information would reveal nonpublic commercial information furnished by the contractor or may be used to reverse engineer the contractor's proprietary technical approach under a government contract.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, signatures, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of specific law enforcement techniques that CBP intends to utilize when
--	--	--	---

			<p>using publicly available social media information in the scope of its law enforcement activities.</p> <ul style="list-style-type: none"> • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Information, such as the quantity and period of performance, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.
Delivery Order 70B04C18F00000377	USCBP000235-41	Released with redactions	<p>Reprocessed with fewer redactions: 000235 (b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include unit prices and ext. prices, where the disclosure of such information would reveal nonpublic commercial information furnished by the contractor or may be used to reverse engineer the contractor's proprietary technical approach under a government contract.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including</p>

			<p>names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Information, such as the delivery date, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.
<p>Contract Number HSHQDC-13-D-00026, Order Number HSBP1017J000831</p>	<p>USCBP000242-49</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000243</p> <p>(b)(3)(A) – Exemption (b)(3)(A) has been applied to records or information that are exempted from disclosure by statute. Redactions applied to this</p>

		<p>information include tax information withheld pursuant to 26 U.S.C. § 6103, which prohibits the disclosure of tax returns or return information.</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include unit prices and ext. prices, where the disclosure of such information would reveal nonpublic commercial information furnished by the contractor or may be used to reverse engineer the contractor's proprietary technical approach under a government contract.</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, signatures, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention</p>
--	--	---

			<p>of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Information, such as the quantity, delivery date, and period of performance, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.
Production 5			
Contract Spreadsheet	USCBP000250	Released with redactions	<p>Reprocessed with fewer redactions: 000250</p> <p>(b)(7)(E) - Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Description of specific technical tools with unique capabilities utilized by CBP to review

			<p>and analyze social media information for law enforcement purposes.</p> <ul style="list-style-type: none"> • Information that would reveal the identity of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Information, such as the quantity and period of performance, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.
<p>Order Number HSBP1014P00537</p>	<p>USCBP000251-71</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000251, 000252, 000253, 000262, 000268</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include:</p> <ul style="list-style-type: none"> • Unit prices and ext. prices, where the disclosure of such information would reveal nonpublic commercial information furnished by the contractor or may be used to reverse engineer the contractor's proprietary technical approach under a government contract. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes</p>

			<p>relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, signatures, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none">• Information, such as the delivery date, that would reveal the degree to which certain law enforcement tools or techniques are available to CBP law enforcement personnel.• Descriptions of specific law enforcement techniques that CBP intends to utilize when using publicly available social media information.• Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.• Descriptions of the scope and investigatory focus of CBP’s operational use of social media.• Names and descriptions of specialized law enforcement units, organizational subunits, and
--	--	--	--

			third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue.
Statement of Work	USCBP000272-84	Released with redactions	<p>Reprocessed with fewer redactions: 000273</p> <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes. • Information, such as the quantity, that would reveal the degree to which certain law

			<p>enforcement tools or techniques are available to CBP law enforcement personnel.</p> <ul style="list-style-type: none"> Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue.
<p>Privacy Threshold Analysis: Office of Information Technology/Cyber Security Directorate, October 10, 2018</p>	<p>USCBP000285-95</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000286, 000293</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include sensitive information about software, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes internal deliberations within DHS consisting of the CBP Privacy Office’s recommendations to the DHS Privacy Office as to the steps necessary to ensure compliance with DHS privacy policies and applicable legal obligations, prior to a final decision of whether to approve a proposed use of social media.</p>

			<p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
Privacy Threshold Analysis: Office of Field Operations, July 8, 2016	USCBP000296- 306	Released with redactions	Reprocessed with fewer redactions: 000297

			<p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include sensitive information about software, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, including descriptions of content and status of draft, pre-decisional documents. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that</p>
--	--	--	---

			<p>would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
--	--	--	---

<p>Privacy Threshold Analysis: Office of Field Operations, August 19, 2016</p>	<p>USCBP000307-15</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000308, 000314</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include: sensitive information about software, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular</p>
--	-----------------------	---------------------------------	--

			<p>individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none">• Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information.• Descriptions of the scope and investigatory focus of CBP’s operational use of social media.• Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue.• Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
--	--	--	--

<p>Privacy Threshold Analysis: Office of Field Operations, November 21, 2016</p>	<p>USCBP000316-26</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000317, 000325</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include sensitive information about software, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Descriptions of analyses being conducted by CBP personnel to evaluate the feasibility and effectiveness of a certain method of using social media information in CBP’s law enforcement and border security mission in order to inform future policy decisions by CBP decision makers. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP.
--	-----------------------	---------------------------------	--

			<p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue.
--	--	--	---

			<ul style="list-style-type: none"> • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes
Privacy Threshold Analysis: Homeland Security Advanced Research Project Agency, November 21, 2016	USCBP000327-36	Released with redactions	<p>Reprocessed with fewer redactions: 000328, 000335</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include sensitive information about software and database, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP.

			<p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none">• Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information.• Descriptions of the scope and investigatory focus of CBP’s operational use of social media.• Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes
--	--	--	---

<p>Privacy Threshold Analysis: Office of Field Operations, May 9, 2017</p>	<p>USCBP000337-48</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000338, 000347</p> <p>(b)(4) - Exemption (b)(4) has been applied to commercial information obtained from a CBP contractor that is privileged or confidential, which the originator of the information would not customarily make available to the public. Redactions applied to this information include sensitive information about software and database, including the type, capabilities and limitations of the software, the business practices of the contractor, and descriptions of how CBP is able to use the software.</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. • Explanations of internal deliberations within DHS, including recommendations from DHS Privacy to CBP. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that</p>
--	-----------------------	---------------------------------	--

			<p>would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p> <p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes
--	--	--	--

<p>Privacy Threshold Analysis: Office of Field Operations, January 5, 2018</p>	<p>USCBP000349-58</p>	<p>Released with redactions</p>	<p>Reprocessed with fewer redactions: 000350, 000356</p> <p>(b)(5) – Exemption (b)(5) has been applied to portions of this intra-agency document that are subject to the deliberative process privilege because the information is predecisional and deliberative and withholding the information is necessary to protect the agency’s decision-making processes. Information redacted under exemption (b)(5) includes:</p> <ul style="list-style-type: none"> • Descriptions of existing or proposed processes for CBP personnel to utilize a certain method of using social media information in CBP’s law enforcement and border security mission in order to inform future policy decisions by CBP decision makers. • Recommendations from the CBP Privacy Office to the DHS Privacy Office prior to the final decision of whether to approve a proposed CBP activity relating to social media, and descriptions of the proposed activity that is pending approval. <p>(b)(6)/(b)(7)(C) - Exemptions (b)(6)/(b)(7)(C) have been applied to information contained in the record, which was compiled for law enforcement purposes relating to the operational use of social media, that would disclose the personal information of a particular individual and disclosure would constitute a clearly unwarranted invasion of personal privacy, including names, phone numbers, and email addresses of non-SES DHS employees.</p>
--	-----------------------	---------------------------------	--

			<p>(b)(7)(E) – Exemption (b)(7)(E) has been applied to information in records compiled for law enforcement purposes, explaining law enforcement techniques and procedures, including information that, either standing alone or combined with other available information, would disclose techniques, procedures, or guidelines for law enforcement investigations and risk circumvention of the law by revealing non-public law enforcement techniques and information. Redacted information includes:</p> <ul style="list-style-type: none"> • Descriptions of specific law enforcement techniques and the types of analysis that CBP does or does not utilize when using publicly available social media information. • Descriptions of the scope and investigatory focus of CBP’s operational use of social media. • Descriptions of criteria for utilizing particular law enforcement techniques, which could reveal the degree to which such techniques are available. • Names and descriptions of specialized law enforcement units, organizational subunits, and third party agencies, the disclosure of which would reveal the investigatory focus of the law enforcement techniques or procedures at issue. • Description of specific technical tools with unique capabilities utilized by CBP to review and analyze social media information for law enforcement purposes.
Withheld in Full			
Email from Office of Chief Counsel	N/A (4 pages)	Withheld in Full	This email was withheld in full under exemption (b)(5).

			Exemption (b)(5) has been applied to attorney/client privileged information. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. The exemption was applied to attorney-client communications.
--	--	--	---

EXHIBIT B



May 24, 2018

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
LEGAL DEPARTMENT**

National Office
125 Broad Street,
18th Floor
New York, NY 10004
Tel: (212) 549-2644
Fax: (212) 549-2644
aclu.org

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA**

39 Drumm Street
San Francisco, CA 94111
Tel: (415) 621-2493
Fax: (415) 255-1478
aclunc.org

FOIA/PA Mail Referral Unit
Department of Justice
Room 115
LOC Building
Washington, D.C. 20530-0001

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

Chief Privacy Officer/Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
245 Murray Lane SW, STOP-0655
Washington, D.C. 20528-0655

FOIA Officer
U.S. Customs & Border Protection
90 K Street NW,
9th Floor, Mail Stop 1181
Washington, D.C. 20229

National Records Center, FOIA/PA Office
U.S. Citizenship & Immigration Services
P. O. Box 648010
Lee's Summit, MO 64064-8010

FOIA Office
U.S. Immigration & Customs Enforcement
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009

U. S. Department of State
Office of Information Programs and Services
A/GIS/IPS/RL
SA-2, Suite 8100
Washington, D.C. 20522-0208

Re: Request Under Freedom of Information Act (Expedited Processing & Fee Waiver/Limitation Requested)

To Whom It May Concern:

The American Civil Liberties Union Foundation and the American Civil Liberties Union Foundation of Northern California (together, the “ACLU”),¹ submit this Freedom of Information Act (“FOIA”) request (the “Request”) for records pertaining to social media surveillance, including the monitoring and retention of immigrants’ and visa applicants’ social media information for the purpose of conducting “extreme vetting.”

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

I. Background

Multiple federal agencies are increasingly relying on social media surveillance to monitor the speech, activities, and associations of U.S. citizens and noncitizens alike.

The Department of Homeland Security (“DHS”) has used social media surveillance for “situational awareness,” intelligence, and “other operations.”² According to documents that the ACLU obtained through FOIA, as of 2015 the DHS Office of Intelligence and Analysis was collecting, analyzing, retaining, and disseminating social media information related to “Homeland Security Standing Information Needs”—subjects on which DHS continuously gathers information.³ A February 2017 report by the DHS Inspector General also confirmed DHS’s use of manual and automated social media screening of immigration and visa applications, the establishment within DHS of a “Shared Social Media Screening Service,” and the planned “department-wide use of

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, educates the public about civil rights and civil liberties issues across the country, directly lobbies legislators, and mobilizes the American Civil Liberties Union’s members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

² Dep’t of Homeland Security, Privacy Impact Assessment of the Office of Operations Coordination and Planning, *Publicly Available Social Media Monitoring and Situational Awareness Initiative 3* (June 22, 2010), available at <https://goo.gl/R1LVxM>.

³ Dep’t of Homeland Security, Office of Intelligence and Analysis, Policy Instruction IA-900, *Official Usage of Publicly Available Information 2* (Jan. 13, 2015), available at <https://goo.gl/6gnmzn>.

social media for screening.”⁴ The same report concluded, however, that DHS lacked the means to evaluate and measure the effectiveness of such programs.⁵ Similarly, internal reviews obtained through FOIA from U.S. Citizenship and Immigration Services show that its social-media screening efforts lacked protections against discrimination and profiling and yielded few actionable results.⁶

Nonetheless, DHS is expanding its social media surveillance efforts as part of the Trump administration’s “extreme vetting” initiatives. The department issued a public notice in September 2017 indicating that the records it retains in immigrants’ files include “social media handles, aliases, associated identifiable information, and search results.”⁷ U.S. Immigration and Customs Enforcement (“ICE”) also solicited proposals from contractors to utilize “social media exploitation” to vet visa applicants and monitor them while they are in the United States.⁸ According to contract documents, ICE plans to spend \$100 million on a program that will employ approximately 180 people to monitor visitors’ social media posts.⁹

The State Department plays a significant role in the collection of social media information for vetting purposes. In May 2017, the department submitted an emergency request to the Office of Management and Budget to expand the information sought from approximately 65,000 visa applicants each year to include, *inter alia*, social media identifiers.¹⁰ On March 30, 2018,

⁴ Office of Inspector General, OIG-17-40, *DHS’ Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success* 1 n.2, 4 (Feb. 27, 2017), available at <https://goo.gl/WDb5iJ>.

⁵ *Id.* at 2.

⁶ See Aliya Sternstein, “Obama Team Did Some ‘Extreme Vetting’ of Muslims Before Trump, New Documents Show,” *Daily Beast*, Jan. 2, 2018, available at <https://goo.gl/azKwLm>.

⁷ Dep’t of Homeland Security, Privacy Act of 1974; System of Records, 82 Fed. Reg. 43,557 (Sept. 18, 2017), available at <https://goo.gl/GcLYoQ>.

⁸ Dep’t of Homeland Security, Immigration & Customs Enforcement, *Extreme Vetting Initiative: Statement of Objectives* §§ 3.1-3.2 (June 12, 2017), available at <https://goo.gl/ZTHzBS>.

⁹ Dep’t of Homeland Security, Acquisition Forecast No. F2018040916 (Apr. 11, 2018), available at <https://goo.gl/Zd7p1p>; see also Drew Harwell & Nick Miroff, “ICE Just Abandoned Its Dream of ‘Extreme Vetting’ Software That Could Predict Whether a Foreign Visitor Would Become a Terrorist,” *Wash. Post*, May 17, 2018, available at <https://goo.gl/UxiF5P>.

¹⁰ Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 20,956 (May 4, 2017), available at <https://goo.gl/2hsRNi>. On August 3, 2017, the State Department notified the public that it would extend the collection of social media information beyond the emergency period. See Sixty-Day Notice of Proposed Information Collection: Supplemental Questions for Visa Applicants, 82 Fed. Reg. 36,180 (Aug. 3, 2017), available at <https://goo.gl/JXTFFi>.

the department signaled a dramatic expansion of its collection of social media information, publishing two notices of new rules which, if adopted, would require nearly all of the 14.7 million people who annually apply for work or tourist visas to submit social media identifiers they have used in the past five years on up to 20 online platforms in order to travel or immigrate to the United States.¹¹ The notices do not indicate how such information may be shared across government agencies or what consequences its collection may have for individuals living in America, including U.S. citizens.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

The Federal Bureau of Investigation (“FBI”) also engages in extensive social media surveillance. In 2012, the FBI sought information from contractors on a planned “social media application” that would enable the FBI to “instantly search and monitor” publicly available information on social media platforms.¹² The FBI revealed in November 2016 that it would acquire social media monitoring software designed by Dataminr that would enable it to “search the complete Twitter firehose, in near real-time, using customizable filters” that are “specifically tailored to operational needs.”¹³ News reports indicate that the FBI is now also establishing a social media surveillance task force, the purpose and scope of which remain unclear.¹⁴

The FBI uses social media surveillance not only “to obtain information about relevant breaking news and events in real-time,” but also to identify subjects for investigation.¹⁵ For instance, it acquired the Dataminr software so that it could identify content that “track[s] FBI investigative priorities.”¹⁶ Similarly, the FBI appears to be using social media as a basis for deciding who to interview, investigate, or target with informants or undercover agents.¹⁷

¹¹ 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13,806 (Mar. 30, 2018), available at <https://goo.gl/Rakt1v>; 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13,807 (Mar. 30, 2018), available at <https://goo.gl/SxJVBk>.

¹² Federal Bureau of Investigation, Strategic Information and Operations Center, Request for Information – Social Media Application (Jan. 19, 2012), available at <https://goo.gl/kRPLZt>.

¹³ Federal Bureau of Investigation, Requisition Number DJF-17-1300-PR00000555, Limited Source Justification, 1 (Nov. 8, 2016), available at <https://goo.gl/Ty9WFZ>.

¹⁴ Chip Gibbons, “The FBI Is Setting Up a Task Force to Monitor Social Media,” *The Nation*, Feb. 1, 2018, available at <https://goo.gl/Ud6mVD>.

¹⁵ *See* FBI, Limited Source Justification, *supra* note 13 at 1.

¹⁶ *See id.*

¹⁷ *See, e.g.*, Center on National Security at Fordham Law, *Case by Case: ISIS Prosecutions in the United States* 19 (July 2016), available at <https://goo.gl/eCE8hh> (concluding that a significant percentage of individuals prosecuted for certain national security-related crimes came to the attention of the FBI through social media use).

Technology plays a critical role in enabling government agencies to surveil and analyze social media content. The migration of speech and associational activity onto the social media web, and the concentration of that activity on a relatively small number of social media platforms, has made it possible for government agencies to monitor speech and association to an unprecedented degree. At the same time, advances in data mining, network analysis, and machine learning techniques enable the government to search, scrape, and aggregate content on a vast scale quickly and continuously, or to focus and filter such content according to specific investigative priorities.

Government surveillance of social media raises serious constitutional and privacy concerns. Most online speech reflects no wrongdoing whatsoever and is fully protected by the First Amendment. Protected speech and beliefs—particularly expression or association of a political, cultural, or religious nature—should not serve as the sole or predominant basis for surveillance, investigation, or watchlisting. When government agencies collect or share individuals’ online speech without any connection to investigation of actual criminal conduct, they foster suspicion about individuals and make it more likely that innocent people will be investigated, surveilled, or watchlisted. Additionally, the knowledge that the government systematically monitors online speech has a deeply chilling effect on the expression of disfavored beliefs and opinions—all of which the First Amendment protects. People are likely to stop expressing such beliefs and opinions in order to avoid becoming the subject of law enforcement surveillance. Basic due process and fairness is also undermined when significant decisions affecting peoples’ lives—such as decisions about immigration status or whether an investigator targets a person for additional scrutiny—are influenced by proprietary systems running secret algorithms, analyzing data without necessary context or rules to prevent abuse. Finally, suspicionless social media surveillance can facilitate government targeting of specific racial and religious communities for investigation and promotes a climate of fear and self-censorship within those communities.

Despite the significant resources federal agencies are expending on social media surveillance and the constitutional concerns it raises, little information is available to the public on the tools and methods agencies use for surveillance, or the policies and guidelines that govern their use. The public similarly lacks information on whether surveillance of social media contributes meaningfully to public safety or simply floods agencies with information on innocent individuals and innocuous conduct. Because government social media surveillance could impact free expression and individual privacy on a broad scale, it has generated widespread and sustained public and media interest.¹⁸

¹⁸ See, e.g., Harwell & Miroff, *supra* note 9; Michelle Fabio, “Department of Homeland Security Compiling Database of Journalists and ‘Media Influencers,’” *Forbes*, Apr. 6, 2018, available at <https://goo.gl/THDSLZ>; Brendan Bordelon, “New Visa Rules Suggest

To provide the public with information on the federal government's use of social media surveillance, the ACLU submits this FOIA Request.

II. Requested Records

- 1) All policies, guidance, procedures, directives, advisories, memoranda, and/or legal opinions pertaining to the agency's search, analysis, filtering, monitoring, or collection of content available on any social media network;
- 2) All records created since January 1, 2015 concerning the purchase of, acquisition of, subscription to, payment for, or agreement to use any product or service that searches, analyzes, filters, monitors, or collects content available on any social media network, including but not limited to:
 - a. Records concerning any product or service capable of using social media content in assessing applications for immigration benefits or admission to the United States;
 - b. Records concerning any product or service capable of using social media content for immigration enforcement purposes;

Expanded Plans for 'Extreme Vetting' Via Algorithm," Nat'l Journal, Apr. 5, 2018, available at <https://goo.gl/9Ux2mX>; Arwa Mahdawi, "Hand Over My Social Media Account to Get a U.S. Visa? No Thank You," Guardian, Mar. 31, 2018, available at <https://goo.gl/tpU6Ba>; Sewell Chan, "14 Million Visitors to U.S. Face Social Media Screening," N.Y. Times, Mar. 30, 2018, available at <https://goo.gl/RDUvKm>; Brendan O'Brien, "U.S. Visa Applicants to be Asked for Social Media History: State Department," Reuters, Mar. 30, 2018, available at <https://goo.gl/3PRMef>; Stephen Dinan, "Extreme Vetting: State Department to Demand Tourists' Social Media History," Wash. Times, Mar. 29, 2018, available at <https://goo.gl/YwazXd>; "U.S. Plans 'Enhanced Vetting' of Every Visa Applicant With Orders to Hand Over Their Social Media History, Old Email Addresses and Phone Numbers," Daily Mail, Mar. 29, 2018, available at <https://goo.gl/yY1g6m>; Gibbons, *supra* note 14; Sternstein, *supra* note 6; Lily Hay Newman, "Feds Monitoring Social Media Does More Harm Than Good," Wired, Sept. 28, 2017, available at <https://goo.gl/4obGFi>; Tal Kopan, "Vetting of Social Media, Phones Possible as Part of Travel Ban Review," CNN.com, Sept. 12, 2017, available at <https://goo.gl/BXf4k3>; Aaron Cantú & George Joseph, "Trump's Border Security May Search Your Social Media by 'Tone,'" The Nation, Aug. 23, 2017, available at <https://goo.gl/MuTmVN>; Conor Finnegan, "Trump Administration Begins Vetting Social Media Profiles for Visa Applicants," ABC News, June 5, 2017, available at <https://goo.gl/cJbnjg>; Russell Brandom, "Can Facebook and Twitter Stop Social Media Surveillance?," Verge, Oct. 12, 2016, available at <https://goo.gl/hzA2fY>; Ron Nixon, "U.S. to Further Scour Social Media Use of Visa and Asylum Seekers," N.Y. Times, Feb. 23, 2016, available at <https://goo.gl/y5C7Ba>.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

- c. Records concerning any product or service capable of using social media content for border or transportation screening purposes;
 - d. Records concerning any product or service capable of using social media content in the investigation of potential criminal conduct;
- 3) All communications to or from any private business and/or its employees since January 1, 2015 concerning any product or service that searches, analyzes, filters, monitors, or collects content available on any social media network;
 - 4) All communications to or from employees or representatives of any social media network (*e.g.*, Twitter, Facebook, YouTube, LinkedIn, WhatsApp) since January 1, 2015 concerning the search, analysis, filtering, monitoring, or collection of social media content; and
 - 5) All records concerning the use or incorporation of social media content into systems or programs that make use of targeting algorithms, machine learning processes, and/or data analytics for the purpose of (a) assessing risk, (b) predicting illegal activity or criminality, and/or (c) identifying possible subjects of investigation or immigration enforcement actions.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), the ACLU requests that responsive electronic records be provided electronically in their native file format, if possible. Alternatively, the ACLU requests that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and that the records be provided in separate, Bates-stamped files.

III. Application for Expedited Processing

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E).¹⁹ There is a “compelling need” for these records, as defined in the statute, because the information requested is “urgen[tly]” needed by an organization primarily engaged in disseminating information “to inform the public concerning actual or alleged Federal Government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

¹⁹ *See also* 6 C.F.R. § 5.5(e); 28 C.F.R. § 16.5(e); 22 C.F.R. § 171.11(f).

- A. *The ACLU is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.*

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute. 5 U.S.C. § 552(a)(6)(E)(v)(II).²⁰ Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the ACLU’s work and are among its primary activities. *See ACLU v. DOJ*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” to be “primarily engaged in disseminating information”).²¹

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to over 980,000 people. The ACLU also publishes regular updates and alerts via email to over 3.1 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to over 3.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,²² and ACLU attorneys are interviewed frequently for news stories about

²⁰ *See also* 6 C.F.R. § 5.5(e)(1)(ii); 28 C.F.R. § 16.5(e)(1)(ii); 22 C.F.R. § 171.11(f)(2).

²¹ Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD*, 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

²² *See, e.g.,* Press Release, American Civil Liberties Union, U.S. Releases Drone Strike ‘Playbook’ in Response to ACLU Lawsuit (Aug. 6, 2016), <https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, Secret Documents Describe Graphic Abuse and Admit Mistakes (June 14, 2016), <https://www.aclu.org/news/cia-releases-dozens-torture-documents-response-aclu-lawsuit>; Press Release, American Civil Liberties Union, U.S. Releases Targeted Killing Memo in Response to Long-Running ACLU Lawsuit (June 23, 2014), <https://www.aclu.org/national-security/us-releases-targeted-killing-memo-response-long-running-aclu-lawsuit>; Press Release, American Civil Liberties Union, Justice Department White Paper Details Rationale for Targeted Killing of Americans (Feb. 4, 2013), <https://www.aclu.org/national-security/justice-department-white-paper-details-rationale-targeted-killing-americans>; Press Release, American Civil Liberties Union, Documents Show FBI Monitored Bay Area Occupy Movement (Sept. 14, 2012), <https://www.aclu.org/news/documents-show-fbi-monitored-bay-area-occupy-movement-insidebayareacom>.

documents released through ACLU FOIA requests.²³

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.²⁴ The ACLU also regularly publishes books, “know your rights” materials, fact sheets, and educational brochures and pamphlets designed to educate the public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily. *See* <https://www.aclu.org/blog>. The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features. *See* <https://www.aclu.org/multimedia>. The ACLU also

²³ *See, e.g.*, Cora Currier, *TSA’s Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, Intercept, Feb. 8, 2017, <https://theintercept.com/2017/02/08/tsas-own-files-show-doubtful-science-behind-its-behavior-screening-program/> (quoting ACLU staff attorney Hugh Handeyside); Karen DeYoung, *Newly Declassified Document Sheds Light on How President Approves Drone Strikes*, Wash. Post, Aug. 6, 2016, <http://wapo.st/2jy62cW> (quoting former ACLU deputy legal director Jameel Jaffer); Catherine Thorbecke, *What Newly Released CIA Documents Reveal About ‘Torture’ in Its Former Detention Program*, ABC, June 15, 2016, <http://abcn.ws/2jy40d3> (quoting ACLU staff attorney Dror Ladin); Nicky Woolf, *US Marshals Spent \$10M on Equipment for Warrantless Stingray Device*, Guardian, Mar. 17, 2016, <https://www.theguardian.com/world/2016/mar/17/us-marshals-stingray-surveillance-airborne> (quoting ACLU staff attorney Nathan Freed Wessler); David Welna, *Government Suspected of Wanting CIA Torture Report to Remain Secret*, NPR, Dec. 9, 2015, <http://n.pr/2jy2p71> (quoting ACLU project director Hina Shamsi).

²⁴ *See, e.g.*, Hugh Handeyside, *New Documents Show This TSA Program Blamed for Profiling Is Unscientific and Unreliable — But Still It Continues* (Feb. 8, 2017, 11:45 AM), <https://www.aclu.org/blog/speak-freely/new-documents-show-tsa-program-blamed-profiling-unscientific-and-unreliable-still>; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA’s Torture Site* (Nov. 22, 2016, 3:15 PM), <https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture>; Brett Max Kaufman, *Details Abound in Drone ‘Playbook’ — Except for the Ones That Really Matter Most* (Aug. 8, 2016, 5:30 PM), <https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most>; Nathan Freed Wessler, *ACLU Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015, 5:30 PM), <https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida>; Ashley Gorski, *New NSA Documents Shine More Light into Black Box of Executive Order 12333* (Oct. 30, 2014, 3:29 PM), <https://www.aclu.org/blog/new-nsa-documents-shine-more-light-black-box-executive-order-12333>; ACLU, *ACLU Eye on the FBI: Documents Reveal Lack of Privacy Safeguards and Guidance in Government’s “Suspicious Activity Report” Systems* (Oct. 29, 2013), https://www.aclu.org/sites/default/files/assets/eye_on_fbi_-_sars.pdf.

publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant Congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.

The ACLU website includes many features on information obtained through the FOIA.²⁵ For example, the ACLU's "Predator Drones FOIA" webpage, <https://www.aclu.org/national-security/predator-drones-foia>, contains commentary about the ACLU's FOIA request, press releases, analysis of the FOIA documents, numerous blog posts on the issue, documents related to litigation over the FOIA request, frequently asked questions about targeted killing, and links to the documents themselves. Similarly, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA and other documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.²⁶

²⁵ See, e.g., Nathan Freed Wessler & Dyan Cortez, *FBI Releases Details of 'Zero-Day' Exploit Decisionmaking Process* (June 26, 2015, 11:00 AM), <https://www.aclu.org/blog/free-future/fbi-releases-details-zero-day-exploit-decisionmaking-process>; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>; *ACLU v. DOJ – FOIA Case for Records Relating to the Killing of Three U.S. Citizens*, ACLU Case Page, <https://www.aclu.org/national-security/anwar-al-awlaki-foia-request>; *ACLU v. Department of Defense*, ACLU Case Page, <https://www.aclu.org/cases/aclu-v-department-defense>; *Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, ACLU Case Page, <https://www.aclu.org/mappingthefbi>; *Bagram FOIA*, ACLU Case Page, <https://www.aclu.org/cases/bagram-foia>; *CSRT FOIA*, ACLU Case Page, <https://www.aclu.org/national-security/csrt-foia>; *ACLU v. DOJ – Lawsuit to Enforce NSA Warrantless Surveillance FOIA Request*, ACLU Case Page, <https://www.aclu.org/aclu-v-doj-lawsuit-enforce-nsa-warrantless-surveillance-foia-request>; *Patriot FOIA*, ACLU Case Page, <https://www.aclu.org/patriot-foia>; *NSL Documents Released by DOD*, ACLU Case Page, <https://www.aclu.org/nsl-documents-released-dod?redirect=cpreirect/32088>.

²⁶ *The Torture Database*, ACLU, <https://www.thetorturedatabase.org>; see also *Countering Violent Extremism FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/cve-foia-documents>; *TSA Behavior Detection FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database>; *Targeted Killing FOIA Database*, ACLU, <https://www.aclu.org/foia-collection/targeted-killing-foia-database>.

The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA requests—the ACLU created an original chart that provides the public and news media with a comprehensive summary index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition, and surveillance.²⁷ Similarly, the ACLU produced an analysis of documents released in response to a FOIA request about the TSA’s behavior detection program²⁸; a summary of documents released in response to a FOIA request related to the FISA Amendments Act²⁹; a chart of original statistics about the Defense Department’s use of National Security Letters based on its own analysis of records obtained through FOIA requests³⁰; and an analysis of documents obtained through FOIA requests about FBI surveillance flights over Baltimore.³¹

The ACLU plans to analyze, publish, and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use and the requesters plan to disseminate the information disclosed as a result of this Request to the public at no cost.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

These records are urgently needed to inform the public about actual or alleged government activity. *See* 5 U.S.C. § 552(a)(6)(E)(v)(II). Specifically, the requested records relate to the federal government’s use of social media surveillance and its interactions with the private sector for the purpose of obtaining social media surveillance technology. As discussed in Part I, *supra*, federal agencies are expanding their use of social media surveillance—which implicates the online speech of millions of social media users—but little information is available to the public regarding the nature, extent, and consequences of that surveillance.

²⁷ *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf.

²⁸ *Bad Trip: Debunking the TSA’s ‘Behavior Detection’ Program*, ACLU (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf.

²⁹ *Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010*, ACLU, <https://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf>.

³⁰ *Statistics on NSLs Produced by Department of Defense*, ACLU (2014), <https://www.aclu.org/other/statistics-nsls-produced-dod>.

³¹ Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), <https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights>.

Given the foregoing, the ACLU has satisfied the requirements for expedited processing of this Request.

IV. Application for Waiver or Limitation of Fees

The ACLU requests a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is “likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.” *See* 5 U.S.C. § 552(a)(4)(A)(iii).³² The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a “representative of the news media” and the records are not sought for commercial use. *See* 5 U.S.C. § 552(a)(4)(A)(ii)(II).

A. The Request is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the ACLU.

As discussed above, credible media and other investigative accounts underscore the substantial public interest in the records sought through this Request. Given the ongoing and widespread media attention to this issue, the records sought will significantly contribute to public understanding of an issue of profound public importance. Because little specific information about government surveillance and monitoring of social media is publicly available, the records sought are certain to contribute significantly to the public’s understanding of whether and under what circumstances the government monitors social media content, and how such monitoring affects individual privacy and liberty.

The ACLU is not filing this Request to further its commercial interest. As described above, any information disclosed by the ACLU as a result of this FOIA Request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress’s legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) (“Congress amended FOIA to ensure that it be liberally construed in favor of waivers for noncommercial requesters.” (quotation marks omitted)).

B. The ACLU is a representative of the news media and the records are not sought for commercial use.

The ACLU also requests a waiver of search fees on the grounds that the ACLU qualifies as a “representative of the news media” and the records

³² *See also* 6 C.F.R. § 5.11(k); 28 C.F.R. § 16.10(k); 22 C.F.R. § 171.16.

are not sought for commercial use. *See* 5 U.S.C. § 552(a)(4)(A)(ii)(II).³³ The ACLU meets the statutory and regulatory definitions of a “representative of the news media” because it is an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” *See* 5 U.S.C. § 552(a)(4)(A)(ii)(III); *see also Nat’l Sec. Archive v. DOD*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, “devises indices and finding aids,” and “distributes the resulting work to the public” is a “representative of the news media” for purposes of the FOIA); *Serv. Women’s Action Network v. DOD*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. DOJ*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington is an entity that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience”); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be “primarily engaged in disseminating information”). The ACLU is therefore a “representative of the news media” for the same reasons it is “primarily engaged in the dissemination of information.”

Furthermore, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to the ACLU’s to be “representatives of the news media” as well. *See, e.g., Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the news media” for purposes of the FOIA); *Nat’l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. DOJ*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a “public interest law firm,” a news media requester).³⁴

On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a “representative of the news media.”³⁵ As was true in those instances, the ACLU meets the requirements for a fee waiver here.

³³ *See also* 6 C.F.R. § 5.11(d)(1); 28 C.F.R. § 16.10(b)(6); 22 C.F.R. § 171.14(b).

³⁴ Courts have found these organizations to be “representatives of the news media” even though they engage in litigation and lobbying activities beyond their dissemination of information / public education activities. *See, e.g., Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 5; *Nat’l Sec. Archive*, 880 F.2d at 1387; *see also Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53-54.

³⁵ In August 2017, CBP granted a fee-waiver request regarding a FOIA request for records relating to a muster sent by CBP in April 2017. In May 2017, CBP granted a fee-

* * *

Pursuant to applicable statutes and regulations, the ACLU expects a determination regarding expedited processing within 10 days. *See* 5 U.S.C. § 552(a)(6)(E)(ii).

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

If the Request is denied in whole or in part, the ACLU asks that you justify all deletions by reference to specific exemptions to FOIA. The ACLU expects the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or deny a waiver of fees.

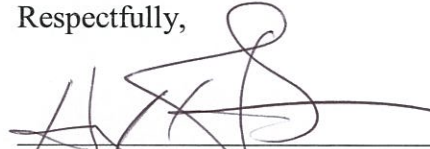
Thank you for your prompt attention to this matter. Please furnish the applicable records to:

Hugh Handeyside
American Civil Liberties Union
125 Broad Street—18th Floor
New York, New York 10004
hhandeyside@aclu.org

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief. *See* 5 U.S.C. § 552(a)(6)(E)(vi).

waiver request regarding a FOIA request for documents related to electronic device searches at the border. In April 2017, the CIA and the Department of State granted fee-waiver requests in relation to a FOIA request for records related to the legal authority for the use of military force in Syria. In March 2017, the Department of Defense Office of Inspector General, the CIA, and the Department of State granted fee-waiver requests regarding a FOIA request for documents related to the January 29, 2017 raid in al Ghayil, Yemen. In May 2016, the FBI granted a fee-waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee-waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to “national security letters” issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ National Security Division granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act. In March 2009, the State Department granted a fee waiver to the ACLU with regard to a FOIA request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists.

Respectfully,

A handwritten signature in black ink, appearing to read 'H. Handeyside', written over a horizontal line.

Hugh Handeyside
American Civil Liberties Union
Foundation

125 Broad Street—18th Floor
New York, New York 10004
212.549.2500
hhandeyside@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Matt Cagle
American Civil Liberties Union
Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
415.621.2493
mcagle@aclunc.org

EXHIBIT C

FOIA Request CBP-2018-058775 Submitted	System	Mr. Hugh Handeyside	05/24/2018	—
--	--------	---------------------	------------	---

This message is to confirm your request submission to the FOIAonline application: View Request . Request information is as follows: Tracking Number: CBP-2018-058775 Requester Name: Hugh Handeyside Date Submitted: 05/24/2018 Request Status: Submitted Description:Please see attached document for further details.

[Copy to Clipboard](#) [Export to CSV](#)

[Previous](#) [1](#) [Next](#)

Other Correspondence Collapse —

Showing 0 to 0 of 0 entries Show entries