

UNCLASSIFIED//FOR OFFICIAL USE ONLY

**MEMORANDUM OF UNDERSTANDING BETWEEN THE
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY AND THE
U.S. DEPARTMENT OF JUSTICE
CHILD EXPLOITATION AND OBSCENITY SECTION**

I. PURPOSE

This memorandum of understanding (MOU) between the Defense Advanced Research Projects Agency (DARPA) and the U.S. Department of Justice Child Exploitation and Obscenity Section (CEOS) defines the data handling procedures the Memex research project will follow regarding the handling, hashing, and transmission of content including text, images, and videos that may be considered obscene or child pornography.

II. BACKGROUND

The DARPA Memex program has been developing computational techniques and software tools for analyzing large volumes of data, both semi-structured (e.g., tabular, relational, categorical, meta-data, and spreadsheets) and unstructured (e.g., text documents and message traffic) that have practical applications in law enforcement investigations and intelligence analysis.

DARPA is expected to benefit under this MOU through opportunities for DARPA performer contractors to develop and transition cutting edge technology using data and problem sets provided by CEOS. CEOS is expected to benefit from technological developments in the Memex program that will improve its data processing operations and software tools.

III. PROPOSED EFFORT/OBJECTIVES

CEOS challenges are similar and relevant to many types of military, law enforcement (LE), and intelligence investigations. Many perpetrators of child pornography crimes maintain a significant presence in like-minded communities on the "dark web" through tools such as Tor, Invisible Internet Project (I2P), and Freenet. CEOS will provide content and subject matter expertise that will enable the DARPA Memex program to develop methods to understand these communities and identify these individuals. CEOS subject matter experts (SMEs) will provide DARPA performer contractors feedback on the utility of their prototype tools to improve operational usage at CEOS.

The proposed activities under this MOU involve CEOS sharing data, problems sets, and user/agent input with DARPA performer contractors for development of technology in Memex and other relevant programs. DARPA will allow Memex contractors to provide expert advice and software tools relevant to CEOS data and problem sets.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Based on the success of cooperation under this MOU, DARPA may, consistent with DoD policy, transition technologies to CEOS.

This MOU does not involve nor authorize intelligence or counterintelligence activities as defined by DoD 5240.1-R, "Activities of DoD Intelligence Components that Affect United States Persons."

This MOU does not involve or authorize human subject research as defined by 32 C.F.R. Part 219 and DoD Instruction 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research," November 8, 2011.

DARPA is a research and development organization and, as such, any tools that result from DARPA activities cannot be certified as error-free for purposes of criminal or civil cases. DARPA expressly disclaims any liability for any consequence regarding the use of the information gleaned from any tools developed by DARPA or its contractors.

All data and problem sets provided by CEOS under this MOU are CEOS records or information. Unless agreed to in writing by both parties, no CEOS data and problem sets will be retained by DARPA performer contractors outside the scope of this MOU. All data provided by CEOS to DARPA performer contractors under this MOU shall be used only to support one or more of the stated objectives of this MOU and shall not be disclosed to any person outside of associated DARPA programs without the prior written permission of CEOS.

IV. CONTENT HANDLING PROCEDURES

As part of the test and evaluation of Memex tools, contractors gather publicly available data for suspected online activities relevant to the CEOS mission. Scrapes of suspected illegal content including text, images, and videos may be conducted by Memex contractors when content is stored on identified public web sites, Tor hidden services, or an approved LE repository maintained by a law enforcement entity such as the Homeland Security Investigations' National Child Victim Identification System. To address this issue, Memex contractors will adhere to the following protocol:

- Tools developed by Memex contractors will access the content stored in computer memory before the content is stored on any permanent storage device to generate different hash values including Message Digest 5 (MD5), Expose F1, and PhotoDNA, or similar one-way image hash functions.
- If Memex contractors have a signed agreement with an approved law enforcement agency to store the suspected illegal content in the law enforcement content repository, Memex contractors will store the suspected illegal content in the approved law enforcement data repository along with the hash values generated by Memex and other identifying information.
- If Memex contractors do not have a signed agreement with a law enforcement agency, their tools will process the content in memory to generate and store hashes

UNCLASSIFIED//FOR OFFICIAL USE ONLY

and other identifying information, but will not store the suspected illegal content on any storage device.

V. RESPONSIBILITIES

DARPA will:

- Direct its contract performers to comply with the protection of all CEOS data and information provided at the necessary classification and privacy levels, while retaining compliance with DoD policies.
- Provide, at the request of CEOS, expert advice through its Memex contract performers and software tools applicable to CEOS-specific problem sets and ongoing cases that may arise during the DARPA-CEOS interaction of research and technology development.
- Comply with DoD and CEOS policies on matters of privacy.

CEOS will:

- Determine what data and problem sets are shared and engage relevant staff for necessary discussions.
- Provide requirements for handling illegal content.
- Support evaluation of the technologies, at various stages of technology development, and provide feedback for further technology refinement.
- Request in writing to DARPA, during the course of research and development, any expert advice, including performer-developed software tools developed during the processing of data relevant to problem sets and ongoing cases.

VI. FUNDING

This MOU does not constitute a commitment of funds between CEOS, DARPA, or any DARPA performer or contractor.

VII. POINTS OF CONTACT

- DARPA: Wade Shen, Program Manager, 571-218-4673, wade.shen@darpa.mil
- CEOS: Damon King, Principal Deputy Chief, (b)(6)@usdoj.gov

VIII. MILESTONES

During the technology development, routine meetings are expected between relevant CEOS-related entities and DARPA. Intermediate technology evaluations are expected to be conducted quarterly, and appropriate staff from both parties will be involved. Every 18 months, DARPA and CEOS will conduct an evaluation of ongoing interactions.

IX. SECURITY

This proposed effort will be protected under the guidance and oversight of the DARPA

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Security and Intelligence Directorate (SID). Depending on the data and context, two levels of classification are expected in this DARPA-CEOS interaction: Unclassified and Unclassified Law Enforcement Sensitive.

X. PUBLIC RELEASE OF INFORMATION

No public affairs requirements are expected for the proposed effort. The DARPA Public Affairs Office and CEOS will coordinate should the need for any releases arise. Information in the custody of DARPA obtained from any data file pursuant to this MOU will be deemed to constitute a record under the control of CEOS for purposes of the Freedom of Information Act, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a.

XI. EFFECTIVE DATE, MODIFICATION, DURATION, AND TERMINATION

The effective date of the MOU is the date of the last signature of approval. Only the authorized signatories to this agreement, or their successors, can approve changes to or the termination of this agreement. Changes will be effective only after both authorized signatories agree to the changes in writing. Either party, or their successors, may terminate this agreement at any time by written notification to the other party, provided such written notification is preceded by consultation between the signatories to the MOU. In the absence of mutual agreement by the authorized officials from CEOS and DARPA, this MOU shall end on December 31, 2017. In the event of early termination, DARPA and CEOS will negotiate the disposition of data and problem sets, tangible assets and liabilities.

XII. DISPUTE RESOLUTION

Any disputes relating to this MOU will, subject to any applicable law, Executive Order, directive or instruction, be resolved by consultation between the parties or in accordance with DoD Instruction 400.19.

XIII. APPROVAL

[Redacted signature box with (b)(6) in the top right corner]

John Lapachbury
Director, Information Innovation Office
Defense Advanced Research Projects Agency

7/15/16
Date

Signature of Steven J. Grocki

Steven J. Grocki
Chief, Child Exploitation and Obscenity Section
U.S. Department of Justice

7/26/16
Date



**MEMORANDUM OF UNDERSTANDING
BETWEEN THE
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
AND THE
DEPARTMENT OF JUSTICE
COUNTERINTELLIGENCE AND EXPORT CONTROL SECTION**

This is a memorandum of understanding (MOU) between the Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O), and the Department of Justice Counterintelligence and Export Control Section and Federal Bureau of Investigation (collectively, Justice). Collectively, DARPA and Justice are referred to as the "Parties."

1. BACKGROUND:

This exchange of analytical information between DARPA and Justice is intended to support the mission of both Parties including but not limited to research and development for the protection of national security and Justice's execution of counterintelligence operations.

2. AUTHORITIES:

- Department of Defense (DoD) Instruction 4000.19, "Support Agreements," April 25, 2013
- DoD Directive 5134.10, "Defense Advanced Research Projects Agency," May 7, 2013
- Executive Order 12333 "United States Intelligence Authorities"
- DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

3. PURPOSE:

This MOU between the Parties establishes responsibilities and objectives for the DARPA Enhanced Attribution program, and other transition opportunities or relevant DARPA program collaborations that may arise during the course of this work.

4. PROPOSED EFFORT / OBJECTIVES:

The Parties will collaborate on further research and evaluation of the Enhanced Attribution program.

5. RESPONSIBILITIES OF THE PARTIES:

DARPA will:

- Provide any relevant information developed from Justice data, including individuals and/or companies believed to be associated with cyber activities of interest.
- Provide Justice with the equipment necessary to transfer data.
- Protect Justice data according to the National Institute of Standards and Technology information security and protection standards.

- Provide Justice with quarterly analytical findings as identified through the use of Justice data until all analysis of Justice-submitted data is complete.
- Recommend to Justice additional analytical tools for data exploitation based on DARPA's analytical findings and research and development initiatives associated with the Enhanced Attribution program and related activities.
- Provide Justice a summary of conclusions based on the findings of its research and the applicability of the Enhanced Attribution program and related activities as a resource to support Justice's cyber mission.
- Refrain from sharing or further distributing Justice data or information derived therefrom (e.g., the results of the analysis of Justice-provided data under the Enhanced Attribution Program and related activities) without the written permission of Justice.

Justice will:

- Provide DARPA with indicators of cyber activity, to be selected at Justice's sole discretion, for analysis using DARPA's Enhanced Attribution program and related activities.
- Work with DARPA as circumstances warrant to evaluate the effectiveness and operational parameters of tools developed through the Enhanced Attribution program.

Due to the need to protect the secrecy and integrity of its criminal investigations, Justice may, at its sole discretion, provide contextual information regarding the indicators of cyber activity that are provided to DARPA. In addition, provide updated or additional collection data as necessary in furtherance of the DARPA and Justice analytical project.

6. PERSONNEL:

Each Party is responsible for all costs of its personnel, including pay and benefits, support, and travel. Each Party is responsible for supervision and management of its personnel.

7. GENERAL PROVISIONS:

Points of Contact (POCs): The following POCs will be used by the Parties to communicate in the implementation of this MOU. Each Party may change its POC upon reasonable notice to the other Party.

- DARPA: Dr. Angelos Keromytis
I2O Program Manager
675 North Randolph Street, Arlington, VA 22203
571-218-4290
angelos.keromytis@darpa.mil

- Justice: (b)(6), (b)(7)(C)
National Security Division, United States Department of Justice
950 Pennsylvania, Ave. NW, Washington, DC 20530
(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)
(b)(7)(E)

[Redacted]

Chief, Cyber Law Unit, Office of General Counsel
Federal Bureau of Investigation
935 Pennsylvania Ave. NW, Washington, DC 20535

(b)(6), (b)(7)(C)
(b)(7)(E)

[Redacted]
(b)(6), (b)(7)(C), (b)(7)(E)

Funds and Manpower: This MOU does not document nor provide for the exchange of funds or manpower between the Parties, nor does it make any commitment of funds or resources.

Modification of MOU: This MOU may be modified only by the written agreement of the Parties, duly signed by their authorized representatives. This MOU will be reviewed annually on or around the anniversary of its effective date, and triennially in its entirety. Each Party shall review the MOU independently. Coordination between Parties is not required unless a change is needed.

Disputes: Any disputes relating to this MOU will, subject to any applicable law, Executive Order, directive or instruction, be resolved by consultation between the Parties or in accordance with DoD Instruction 4000.19.

Termination of Understanding: This MOU may be terminated in writing at will by either Party.

Effective Date: This MOU takes effect the day after the last Party signs. The signatories to this agreement, or their successors, will approve all changes to or the termination of this agreement. Changes are effective only after both signatories, or their successors, agree to the changes in writing. Subject to a reasonable determination that the program will not produce beneficial results commensurate with the expenditure of resources, the Parties may terminate this agreement through written notification, provided such written notification is preceded by consultation between the signatories, or their successors, to the MOU. In the event of early termination, the Parties will negotiate the disposition of tangible assets and liabilities.

Expiration Date: This MOU expires on May 18, 2021.

Schedule / Milestones: The Parties will coordinate on an ad hoc basis as the Enhanced Attribution program develops.

8. SECURITY:

The Enhanced Attribution program will be protected under the guidance and oversight of the DARPA Security and Intelligence Directorate (SID) and DARPA's Original Classification Authority. The planned program efforts associated with this MOU will be conducted at the UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY levels. DARPA SID is responsible for foreign disclosure decisions on this program.



9. PUBLIC RELEASE OF INFORMATION:

DARPA will remain the office of primary responsibility for external relations (public and congressional affairs) for matters pertaining to the Enhanced Attribution program. All external requests for information regarding the Enhanced Attribution program will be submitted to DARPA's Public Affairs Office, which has sole responsibility for public release authorization determinations regarding Enhanced Attribution while the program is managed by DARPA. All data, information, and documentation related to Enhanced Attribution generally intended for external release must be submitted to the DARPA Public Release Center for Distribution Statement A approval. As set forth in Section 5 above, all data, information, and documentation related the Justice-provided data, or Enhanced Attribution Program data derived therefrom, cannot be released by the DARPA Public Release Center without the express written consent of Justice.

10. APPROVAL:

 (b)(6)

Brian M. Pierce
Director, Information Innovation Office
Defense Advanced Research Projects Agency

9 JUNE 2017
Date

 (b)(6), (b)(7)(C)

Counterintelligence and Export Control Section
National Security Division
U.S. Department of Justice

6/19/2017
Date

