January 16, 2014

Office of the Secretary of Defense / Joint Staff
FOIA Requester Service Center
1155 Defense Pentagon
Washington, D.C. 20301-1155

US Strategic Command (STRATCOM)
J006 / FOIA Requester Service Center
901 Sac Blvd. Ste. 2E27
Offutt Air Force Base, NE 68113-2040

US Special Operations Command (USSOCOM)
SOCS-SJS-I / FOIA Requester Service
7701 Tampa Point Blvd.
MacDill Air Force Base, FL 33621-5323

US Central Command (CENTCOM)
CCJ6-RDF / FOIA Requester Service
7115 South Boundary Blvd.
MacDill Air Force Base, FL 33621-5101

US Europe Command (EUCOM)
Unit 30400 APO AE 09131 / FOIA Requestor Service
2308 Gebaude, Patch Barracks, Stuttgart-Vaihingen, Germany 70569

US Africa Command (AFRICOM)
Unit 29951 APO AE 09751 / FOIA Requester Service
Kelley Barracks, Stuttgart-Moehringen, Germany 70435

Defense Intelligence Agency
DAN-1A / FOIA Requester Service
200 MacDill Blvd.
Bolling Air Force Base, Washington, D.C. 20340-5100

Defense Contract Audit Agency
Attn: Mr. Merrick Krause, FOIA Public Liaison
8725 John J. Kingman Road, Suite 2135
Fort Belvoir, VA 22060-6219

National Security Agency / Central Security Service (NSA/CSS)
N5P5 / FOIA Requester Services
9800 Savage Road, Suite 6248, Fort George G. Meade, MD 20755–6248

Re: REQUEST UNDER THE FREEDOM OF INFORMATION ACT

To Whom It May Concern:

This letter constitutes a request under the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"), and the Department of Defense implementing regulations, 32 C.F.R. § 286. The request is submitted by the American Civil Liberties Union and the American Civil Liberties Union Foundation (together, "the ACLU" or "requester"),[1] and seeks the release of records that describe the Defense Department's authority to engage in "influence activities," the use of deception, and the use of misattributed or unattributed communications on the Internet.

I. Background

The Internet has opened up unprecedented opportunities for influence and deception by the U.S. government and military. Formerly known as "PsyOps," and recently rebranded as "Military Information Support Operations," or "MISO," military propaganda has traditionally been considered too anti-democratic to deploy against American targets. With the advent of the web, however, the distinction between foreign and American audiences has become increasingly blurred. Without access to the policies and procedures guiding the Defense Department's MISO and other information activities, Americans who read, congregate, network, and play online may become the unwitting consumers—or targets—of influence and deception operations by their own military.

Recent events demonstrate that outside contractors engaging in communications support for the military are unrestrained by the prospect that their online "information operations" will shape American opinions and lives. Last summer, Somali-American Abdiwali Warsame became the target of a proposal to undercut his wide Internet following by planting critical readers' comments on his website after he was tagged as an "extremist" by a defense contractor hired to "counter nefarious influences" in Africa.[2] In 2012, an owner of a military contracting firm admitted to misattributing blog and Wikipedia content, setting up "false" Twitter and Facebook accounts, and registering "fake" websites as part of a plot to discredit two *USA Today* journalists in retribution for exposés about his company's "information support" activities in Iraq and Afghanistan.[3]

The year's disclosures of the government's post-9/11 surveillance activities confirm that its interests in Internet surveillance extend beyond collection of communications. In November,

[1] The American Civil Liberties Union is national organization that works to protect civil rights and civil liberties. Among other things, the ACLU advocates for national security policies that are consistent with the Constitution, the rule of law, and fundamental human rights. The ACLU also educates the public about U.S. national security policies and practices including, among others, government transparency and accountability; cybersecurity and digital rights; the domestic surveillance programs; racial and religious discrimination and profiling; and the human costs of war and counterterrorism programs.

[2] Craig Whitlock, *Somali American Caught Up in a Shadowy Pentagon Counterpropaganda Campaign*, WASH. POST, July 7, 2013, http://www.washingtonpost.com/world/national-security/somali-american-caught-up-in-a-shadowy-pentagon-counterpropaganda-campaign/2013/07/07/b3aca190-d2c5-11e2-bc43-c404c3269c73_story.html.

[3] Gregory Korte, *Propaganda Firm Owner Admits Attacks on Journalists*, USA TODAY, May 25, 2012, http://usatoday30.usatoday.com/news/military/story/2012-05-24/Leonie-usa-today-propaganda-pentagon/55190450/1.

journalist Glenn Greenwald disclosed the National Security Agency's proposal to build secret dossiers on the private Internet lives of critics of U.S. policy deemed Muslim "radicalizers"—including sexual communications and visits to pornographic websites—to be used for sabotaging their reputations and online influence.[4] In December, ProPublica revealed that the Defense Humint Service and the DIA, along with other intelligence agencies, had populated interactive fantasy games with so many avatars that a "deconfliction" group was needed to avert gaming between undercover agents.[5] To the intelligence agencies, popular gaming platforms like World of Warcraft and Second Life offered an "opportunity" to impart a "targeted message or lesson" from "the Western point of view."[6] Developing an "in-game presence," advised a potential contractor, would allow agents to identify "propaganda efforts in the game space," work with the game producer to eliminate "harmful or misleading information," and use their avatars' influence to replace this content with "counterpropaganda" of their own.[7]

As influence activities migrate to an online "information environment" without borders, the permanence of conventional checks on the domestic use of military propaganda is being called into question. Department newsletters have highlighted the repeal of the Smith-Mundt Act, a statutory ban on domestic broadcasts by the State Department long presumed also to bind the military.[8] And as discussed above, recent reports confirm that influence activities on the web—particularly those conducted by defense contractors—have indeed targeted American citizens and influenced American audiences.

Despite these concerns, the parameters of the DOD's Strategic Communications ("SC") and Information Operations ("IO") programs, and the legal basis for restricting their use on Americans, remain obscure. Denying Americans access to government messages disseminated in their name contravenes fundamental values of speech, accountability, and open democracy.[9] But the covert use of military propaganda by a state to disgrace or deceive its own citizens also threatens democratic principles. Far more transparency is needed regarding how the U.S. government uses the troves of intelligence gleaned from Internet surveillance; when it may disseminate information for worldwide consumption through avatars and fictitious online

---

[4] Glenn Greenwald, Ryan Gallagher & Ryan Grim, *Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit 'Radicalizers,'* HUFF. PO., Nov. 26, 2013, http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html.

[5] Justin Elliott, PROPUBLICA, & Mark Mazzetti, N.Y. TIMES, *World of Spycraft: NSA and CIA Spied in Online Games*, Dec. 9, 2013, http://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games.

[6] Unattributed, Exploiting Terrorist Use of Games & Virtual Environments 2, in "Top Secret" memorandum dated Jan. 8, 2007, derived from NSA/CSSM 1-52, *available at* CRYPTOME.ORG, http://cryptome.org/2013/12/nsa-spy-games.pdf (last visited Jan. 3, 2014).

[7] SCIENCE APPLICATIONS INTERNATIONAL CORPORATION (SAIC), GAMES: A LOOK AT EMERGING TRENDS, USES, THREATS AND OPPORTUNITIES IN INFLUENCE ACTIVITIES 61–63 (undated), *available at* EFF.ORG, https://www.eff.org/files/2013/12/09/20131209-nyt-nsa_games.pdf (last visited Jan. 11, 2014).

[8] The House Armed Services Committee recently ordered the DOD to review its interpretation of the Smith-Mundt Act's domestic dissemination ban as applied to DOD online messaging, noting that the "overly cautious" Department interpretation "may inhibit more aggressive strategic communications against our adversaries abroad." H.R. Rep. No. 111-166, at 376–77 (2009), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-111hrpt166/pdf/CRPT-111hrpt166.pdf (last visited Jan. 11, 2013).

[9] *Compare Essential Info., Inc. v. U.S. Info. Agency*, 134 F.3d 1165, 1170 (D.C. Cir. 1998) (broadcasts of the U.S. Information Services (USIA) exempt from FOIA disclosure because of Smith-Mundt Act's "domestic propaganda" ban).

personas; and when the DOD and military may use MISO techniques to manipulate, disgrace, or deceive.

II. Requested Records

Accordingly, the ACLU seeks disclosure of the following records:

A. Information and influence on social media and interactive gaming websites

1. Policies, procedures, and practices regarding the use of Strategic Communications ("SC"), Information Operations ("IO"), and other information and influence activities on "social media platforms" or "social networking websites."

The terms "social media platforms" and "social networking websites" should be construed to encompass all online platforms, communities, apps, and websites used to congregate, interact, connect, or share, including but not limited to Wikipedia, Myspace, Facebook, LinkedIn, Google+, Tumblr, Twitter, Foursquare, Etsy, Flickr, Reddit, blogs, listservs, website RSS feeds, specialized forums associated with gaming and dating platforms, etc.

2. Policies, procedures, and practices regarding the use of SC, IO, and other information and influence activities on Games and Virtual Environments (GVEs).

The term "GVE" should be construed to encompass all online games and gaming platforms, multi-user virtual worlds and massively multiplayer online (MMO) games such as Second Life, the Sims Online, HiPiHi, Kaneva, Gaia Online, City of Heroes, There.com, Entropia Universe, Everquest, Final Fantasy, Dungeons and Dragons Online, Special Forces and SF2, Xbox Live, World of Warcraft, Under Siege, Words With Friends, etc.

3. Policies, procedures, and practices governing SC, IO, and other information and influence activities on social media platforms, social networking websites, or GVEs (collectively, "online content and accounts"), used by or accessible to United States audiences.

The term "United States audiences" should be construed to encompass all U.S. persons, including media companies and elected officials.

B. Attribution and deception on social media and interactive gaming websites

1. Policies, procedures, and practices governing source attribution, misattribution, or non-attribution of online content and accounts, including those governing use of "avatars," attribution to fictitious identities, or attribution to U.S. or non-U.S. persons, living or dead, not actually engaged in SC, IO, or other information or influence activities on behalf of the government.

2. Policies, procedures, and practices governing the use of technology for automatically generating online content and accounts, and policies, procedures,

and practices governing the use of technology for commanding a unit of actual or fictitious online identities ("Persona Management Software").

3. Policies, procedures, and practices governing the dissemination of disinformation or deception by the use of online content and accounts.

The terms "disinformation" and "deception" should be construed to encompass any content or communicative conduct deliberately inaccurate or untrue in fact or intent, including content or conduct used to discredit truthful or accurate information; to generate a target audience's false conclusions about accurate information; or to mislead a target audience as to the capabilities, intentions, and operations of the United States military or government or of friendly or adversary militaries or governments.

C. Legal interpretations of information and influence authorities

1. Any orders, opinions, interpretations, or memoranda expressing the legal position of the Department of Defense regarding the authority to engage in SC, IO, and other information and influence activities on the Internet;

2. Any orders, opinions, interpretations, or memoranda expressing the reasons and basis for any Department of Defense or military policies limiting the use of:

(a) SC, IO, and other information and influence activities in online content accessible to U.S. audiences;

(b) disinformation or deception in online content accessible to U.S. audiences; and

(c) misattribution or non-attribution of online content or accounts used by or accessible to U.S. audiences.

3. Any orders, opinions, interpretations, memoranda, or working law regarding the legal repercussions of 22 U.S.C. §§ 1461-1a & 1462 (amending the Smith-Mundt Act), with respect to the use of SC, IO, and other information and influence activities by the Department of Defense and components of the U.S. military.

D. Compartmentalization, training, and oversight

1. Any reports or documentation of noncompliance with respect to the policies, procedures, and practices governing SC, IO, and other information and influence activities by the United States or its contractors, and any remedial actions taken with respect thereto.

2. Any records, reviews, or reports issued by the Information Operations Executive Steering Group (IO ESG) or the Strategic Communication Integration Group Executive Committee (SCIG EXCOM).

3. Policies, procedures, practices, guidance, and training materials provided to contract employees engaged in SC, IO, or other information and influence activities regarding:

(a) source attribution, misattribution, or non-attribution;

(b) disinformation or deception; and

(c) use of content or accounts used by or accessible to U.S. audiences.

4. Policies, procedures, and practices regarding the attribution of Defense Department- or military-generated SC, IO, and other information and influence activities to other agencies or governments.

5. Policies, procedures, and practices regarding the use of SC, IO, and other information and influence activities by public affairs, public relations, or media relations personnel in the Department of Defense and the military components, or policies, procedures, and practices regarding the placement of such personnel within chains of command that may engage in or supervise SC, IO, or other information and influence activities.

III. Request for a Fee Limitation and Public Interest Fee Waiver

The ACLU requests a waiver of search and review fees because the requested records are not sought for commercial use and because the ACLU is a "representative of the news media." 5 U.S.C. § 552(a)(4)(A)(ii)(II). Dissemination of information about actual or alleged government activity is a critical and substantial component of the ACLU's mission and work. The ACLU disseminates this information to educate the public and promote the protection of civil liberties. Its regular means of disseminating and editorializing information obtained through FOIA requests include: a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers; published reports, books, pamphlets, and fact sheets; a widely read blog; heavily visited websites, including an accountability microsite, http://www.aclu.org/accountability; and a video series.

The ACLU therefore meets the statutory definition of a "representative of the news media" as 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." 5 U.S.C. § 552(a)(4)(A)(ii).[10] Indeed, the ACLU recently was held to be a "representative of the news media."[11]

The ACLU also requests a waiver of all search, review, or duplication fees on the ground that disclosure of the requested information is in the public interest because: (1) it "is likely to contribute significantly to public understanding of the operations or activities of the government," and (2) it "is not primarily in the commercial interest of the requester." 5 U.S.C. §

[10] *See also Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group to be "'primarily engaged in disseminating information'").

[11] *Serv. Women's Action Network v. Dep't of Defense*, 888 F. Supp. 2d 282, 287–88 (D. Conn. 2012); *see also Am. Civil Liberties Union of Wash. v. Dep't of Justice*, No. C09–0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a "representative of the news media"), *reconsidered in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).

552(a)(4)(A)(iii). This request clearly satisfies these criteria.

For these reasons, we respectfully request that all fees related to the search, review, and duplication of the requested records be waived. If the search and review fees will not be waived, we ask that you contact us at the email address listed below should the estimated fees resulting from this request exceed $100.

We request that responsive electronic records be provided electronically in their native file format, if possible. *See* 5 U.S.C. § 552(a)(3)(B). Alternatively, we request 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 in separate, Bates-stamped files.

We also request that you provide an estimated date on which you will finish processing this request. *See* 5 U.S.C. § 552(a)(7)(B).

If this FOIA request is denied in whole or in part, please provide the reasons for the denial, pursuant to 5 U.S.C. § 552(a)(6)(A)(i). In addition, please release all segregable portions of otherwise exempt material in accordance with 5 U.S.C. § 552(b). Furthermore, if any documents responsive to this request are classified, please identify those documents, including a date and document number where possible, so we may begin the process of requesting a Mandatory Declassification Review under the terms of Executive Order 13,526 (2010).

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact us at the email address listed below. Pursuant to 5 U.S.C. § 552(a)(6)(A)(i), we expect a response regarding this request within the twenty working-day statutory time limit.

Sincerely,

/s/ *Lee Rowland*
Lee Rowland
Senior Staff Attorney
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
lrowland@aclu.org

/s/ *Rita Cant*
Rita Cant
Brennan Fellow
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
rcant@aclu.org