



OVERWATCH

*"The advancement and diffusion of knowledge is the only guardian of true liberty."
-James Madison*



THE JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume 3 · Issue 3 · September 2014



Photo By: Sgt. Frances Johnson

IN THIS ISSUE: Feature Article - *Privacy Watchdog's Next Target*



Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) will promote Marine Corps combat readiness, institutional integrity, effectiveness, discipline, and credibility through impartial and independent inspections, assessments, inquiries, investigations, teaching, and training.

The Intelligence Oversight Division

To ensure the effective implementation of Marine Corps-wide oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and Special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Contact Information

Mail:

Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director
Maj Christopher L. Doyle, Deputy Director
Maj Harold R. Henderson, Sensitive Activities

Inside This Issue

Features

- 3 A Message from the Director
- 4 Privacy Watchdog's Next Target: The Least-Known but Biggest Aspect of NSA Surveillance
- 6 Is There a Second NSA Leaker After Snowden?
- 7 Intelligence Photographs in the News



Web Links

Assistant to the SECDEF for Intel Oversight (ATSD-IO)
<http://atsdio.defense.gov/>

Marine Corps Inspector General
<http://www.hqmc.marines.mil/igmc/UnitHome.aspx>

Naval Inspector General
<http://www.ig.navy.mil/>

Message from the Director, Intelligence Oversight

I would like to start off by thanking everyone for their comments and feedback to our recent newsletters. The goal of this quarterly periodical is to keep our Marine Corps intelligence professionals aware of updates in the world of oversight. I would also like to extend kudos to my deputy, **Major Chris Doyle** for getting this newsletter out in a timely manner. As a short staffed directorate of the Office of Inspector General, my visits to you in the fleet are sporadic at best. As funding becomes available, I will increase our visits to your unit to hear your concerns and issues. My goal is to be able to relay those concerns to HQMC leadership and hopefully spark discussions that lead to resolution.

As you read this newsletter, you will see that privacy continues to be on the forefront. The National Security Agency continues to get flak over their collection program. Additionally, there is potential fallout from another “Snowden type leaker which remains to be seen. Presidential Policy Directive 19 regarding the Protection of Whistleblowers with access to Classified Information continues to be a hot topic, particularly in the Inspector General realm.

As a reminder, please note that the IGMC has a location on the classified USMC web portal to allow receipt of classified complaints on the Inspector General website. This will ensure that everyone has a classified means to provide a complaint that will remain within the classified realm. We want to ensure that if there is a complaint, we keep it relegated to the proper systems to prevent a spillage. Earlier this month I traveled to Darwin Australia to meet with your intelligence Marines located with Marine Rotational Force-Darwin. With a small staff, they are gainfully employed with our Australian counterparts and setting the bar high for follow on units.



In this month’s feature article, “Privacy Watchdog’s Next Target: The Least-Known but Biggest Aspect of NSA Surveillance,” the authors report about concerns a privacy advocate group has with Executive order 12333. Specifically, they take issue with the overseas collection of U.S. persons’ data. Regardless of the outcome of this specific examination, we should be reminded that there continues to be a ‘trust-gap’ between the intelligence community and the population at-large. It is important to ensure we are doing all we can to protect the rights and privacy of our nation’s citizens. Additionally, when language appears ambiguous, we should ensure we start a dialogue involving your Commanding Officer, Staff Judge Advocate, and my office if necessary to ensure we make the right decisions, while not impeding on others’ civil liberties.

As always, in order to continue providing information on the most important and relevant oversight issues, I am requesting that our intelligence professionals continue to submit ideas for future topics of interest that you feel would benefit the Marine Corps Intelligence Community as well as any comments or feedback. Please provide them directly to my deputy at christopher.l.doyle@usmc.mil.

I continue to be impressed at the professionalism and knowledge of our Intelligence Marines I meet as I travel around the fleet. Please continue to be engaged and keep up the great work.

Semper Fidelis
Edwin T. Vogt
Director, Intelligence Oversight Division
Office of the Inspector General of the Marine Corps
Ph: 703-604-4518 DSN: 664-4518 Email: Edwin.Vogt@usmc.mil

Feature Article

Privacy Watchdog's Next Target: The Least-Known but Biggest Aspect of NSA Surveillance

By Ellen Nakashima and Ashkan Soltani

An independent privacy watchdog agency announced Wednesday that it will turn its focus to the largest and most complex of U.S. electronic surveillance regimes: signals intelligence collection under Executive Order 12333.

That highly technical name masks a constellation of complex surveillance activities carried out for foreign intelligence purposes by the National Security Agency under executive authority. But unlike two other major NSA collection programs that have been in the news lately, EO 12333 surveillance is conducted without court oversight and with comparatively little Congressional review.

The Privacy and Civil Liberties Oversight Board, an independent executive branch agency, over the last year has taken in-depth looks at the other two NSA programs. It concluded the bulk collection of Americans' phone call metadata under Section 215 of the Patriot Act was illegal and raised constitutional concerns. By contrast, it found the gathering of call and email content under Section 702 of the Foreign Intelligence Surveillance Act to be lawful, though certain elements pushed "close to the line" of being unconstitutional.

Now the board is planning to delve into EO 12333 collection, among other topics. It is not clear, however, how deep or broad its examination will be.

"It's obviously a complex thing to look at 12333," but "it's something we'll likely be delving into," said a member of the Privacy and Civil Liberties Oversight Board who requested anonymity in order to speak freely. The board has highlighted 12333 issues in the past. For example, each agency is supposed to have guidelines to carry out the executive order, but some guidelines are three decades old. The board has encouraged the guidelines be updated, the source said.

Collection outside the United States has attained new relevance given media reports in the last year about broad NSA surveillance based on documents leaked to journalists by former agency contractor Edward Snowden.

"Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215," said a former State Department official, John Napier Tye, in an op-ed published Sunday in The Washington Post.

Issued in 1981 by President Ronald Reagan, EO 12333 laid out the roles and powers of the various intelligence agencies. It specified that the NSA had control of signals intelligence collection for foreign intelligence and counterintelligence purposes. But the nature and scope of the collection activities have not been clarified for the public.

Unlike surveillance inside the United States or which targets U.S. citizens and legal residents, collection under 12333 does not require a warrant. Once upon a time, you could be fairly certain that overseas collection would pick up only foreigners' phone calls and that Americans' communications would stay inside the United States. But today, emails, calls and other communications cross U.S. borders and are often stored beyond them. Companies like Google and Yahoo have "mirror" servers around the world that hold customers' data. That means Americans' data are often stored both in the United States and abroad simultaneously, subject to two different legal and oversight regimes. Surveillance on U.S. soil requires court permission and an individual warrant for each target.

Surveillance abroad requires a warrant for U.S. persons, but if collection is coming from a data center overseas, large volumes of Americans' communications may be picked up as "incidental" to collection on a foreign target. "So a lot of ordinary data crosses borders, including domestic communications between Americans," said Edward W. Felten, a computer science professor at Princeton University. Or as former NSA Deputy Director John C. Inglis has said of the falling away of borders in

cyberspace: “There is not an away game. There is not a home game. There is only one game.” With the merging of the home and away games, the question arises as to whether a legal regime that bases privacy protections and oversight largely on geography is sufficient, analysts say.

The Post reported last fall, for example, that NSA was collecting 500,000 e-mail accounts “address books” a day outside the United States from companies such as Yahoo and Google. According to documents obtained from Snowden, the agency was collecting the data through secret arrangements with foreign telecommunications companies or allied intelligence services in control of facilities that direct traffic along the Internet’s main data routes. Although the collection takes place overseas, two senior U.S. intelligence officials acknowledged that it “incidentally” sweeps in the contacts of many Americans, the article said. The Post also reported that the agency in conjunction with Britain’s GCHQ, was collecting data traveling between Google and Yahoo data centers overseas. In Google’s case, that was up to 6 million records a day, according to a slide obtained from Snowden. The firms have since said they are encrypting the data moving between their data centers.

EO 12333 collection is not available everywhere in the world, former U.S. officials said. It is not as precise as collection from a U.S. carrier in the United States, which can filter out unwanted communications. Under 12333, the agency is “collector and processor,” said one former U.S. official, who spoke on condition of anonymity to discuss a sensitive topic. “Things go by and you now have to figure out which things are of interest to you.” And those things are “incredibly fractured and packetized.”

Tye said before he left the State Department, he filed a complaint with its inspector general, as well as the NSA inspector general, alleging that 12333 collection through its “incidental collection” of Americans’ data, violated the Fourth Amendment’s bar on unreasonable searches and seizures. “Basically 12333 is a legal loophole,” said Tye, who is now legal director at Avaaz, a civil society group working on regional and national issues ranging from corruption and poverty to conflict and

climate change. “It allows the NSA to collect all kinds of communications by Americans that the NSA would not be able to collect inside the borders” without a warrant.

Inglis said Tye’s description of 12333 as a loophole is “simply wrong, in both fact and spirit.” Said Inglis: “There are no ‘rules free’ zones at NSA and the responsibility to ensure the privacy rights of U.S. persons conveyed across all facets of the signals intelligence cycle, from collection to dissemination.”

Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society, said 12333 allows “bulk collection” of data or the ingestion of massive amounts of data without a filter for a target’s e-mail address or phone number, for instance.

“Both collection and use are far less regulated” than collection inside the United States, she said. “We don’t know how or how much information is collected, used, analyzed or shared.”

At the same time, she said, “while 12333 greatly affects Americans and other people from all over the world, the public and Congress are basically in the dark about what the NSA is doing.”

NSA Spokeswoman Vanee Vines said that “whether NSA’s activities are conducted under EO 12333 or the Foreign Intelligence Surveillance Act [which governs domestic surveillance], NSA applies attorney general-approved processes to protect the privacy of U.S. persons in the collection, retention and use of foreign intelligence.”

She added that President Obama issued additional guidance in January under Presidential Policy Directive 28, which provides that such activities “shall be as tailored as feasible.”

The directive specified that “appropriate safeguards be applied to protect the personal information of all individuals, regardless of nationality.”

A fundamental unresolved question is this: At what point should these privacy safeguards kick in? At the point the data are swept in by the intelligence agency or when they are plucked out for analysis and sharing with other agencies?

Currently, they apply once the data are processed, former officials said.

The privacy protections governing 12333 collection are in US Signals Intelligence Directive 18. That NSA policy document, for instance, states that communications to, from or about U.S. persons collected under the authority may be retained for five years, unless the NSA director determines a longer period is required.

It also states that they may be kept for a "period sufficient" if they are reasonably believed to become relevant to a current or future foreign intelligence requirement. Or if the information provides evidence of a crime, in which case it may be shared with the relevant agency.

Such qualifications, privacy advocates have said, amount to "loopholes" that enable the retention of large amounts of U.S. persons' data.

One thing is clear: examining overseas collection under 12333 "is a massive undertaking," the board source said. But "it is something we have to look at."

Soltani is an independent security researcher and consultant.

Is There a Second NSA Leaker After Snowden?

By Julian Hattem

Top experts say there could be a new person leaking details about the National Security Agency, in addition to former contractor Edward Snowden. Glenn Greenwald, the journalist most closely associated to Snowden, said he suspects someone else has been involved in leaking out new documents, and other experts have backed up the claim. The existence of a second leaker "seems clear at this point," Greenwald wrote on Twitter over the weekend.

"The lack of sourcing to Snowden on this & that last [Der Spiegel] article seems petty telling," he added, after German broadcasters reported that the NSA was tracking people searching for details about privacy software. Neither the Der Spiegel article from December nor last week's story, both of which were partly written by privacy advocate and security researcher Jacob Appelbaum, specifically mentioned that the information emanated from leaks by Snowden.

"That's particularly notable given that virtually every other article using Snowden documents - including der Spiegel - specifically identified him as the source," Greenwald said in an email to The Hill on Monday. Other people who have seen Snowden's trove of documents have agreed that the documents revealed by German outlets seem to indicate a second source.

Bruce Schneier, a cryptologist and cybersecurity expert who has helped the Guardian review Snowden's disclosures, said he did "not believe that this came from the Snowden documents."

"I think there's a second leaker out there," he wrote in a blog post last week.

If true, it could add another headache for the NSA, which has struggled for more than a year to contain the fallout from Snowden's revelations. Defenders of the NSA say that the disclosures have hurt U.S. security and empowered terrorists and other enemies abroad. Among other internal reforms, the spy agency has beefed up its clearance procedures to prevent another employee from passing along secret documents to journalists or governments in Beijing and Moscow. "If in fact this is a post-Snowden NSA leak, then it's probably just proof that you can always build a bigger mousetrap; that doesn't mean you're going to catch the mice," said Stephen Vladeck, a law professor at American University who specializes in national security issues.

Vladeck added that leaks about controversial national security programs are in many ways inevitable, and may not be tied to Snowden's leaks in any way.

For Greenwald, however, a second leaker would be affirmation of Snowden's actions. "I've long thought one of the most significant and enduring consequences of Snowden's successful whistleblowing will be that he will inspire other leakers to come forward," he told The Hill.

Intelligence Photographs in the News



Marine Corps Air Station Futenma - Okinawa, Japan - Corporal Cody C. Kurfman speaks with maintenance engineers with the Japan Ground Self Defense Force at Marine Corps Air Station Futenma, July 18. The JGSDF engineers viewed a static display of an MV-22 Osprey with Marine Medium Tilt rotor Squadron 262 (Reinforced), 31st Marine Expeditionary Unit. They learned about the Osprey's capabilities and took a tour through the aircraft before visiting an AH-1W Cobra and a UH-1Y Huey. Kurfman is a special communications signals analyst with 3rd Intelligence Battalion, 3rd Marine Expeditionary Force Headquarters Group, III MEF, and a native of Nara Prefecture, Japan. *Photo By: Cpl. Henry Antenor*

Constanta, Romania - First Lt. Adam Fountain, a ground intelligence officer with Black Sea Rotational Force 14, from 3rd Battalion, 8th Marine Regiment, shows children the inside of a medical Humvee while Marines and sailors visited a local park in Constanta, Romania during Children's Day weekend with the community May 31, 2014. Marines and sailors participated in Romania's Children's Day with a showcase of standard-issued equipment and military vehicles for children to interact with first-hand. The observation promotes mutual exchange and understanding among children while encouraging actions to benefit and promote the welfare of the nation's children.

Photo By: Cpl. Scott W. Whiting



KABUL, Afghanistan (Aug. 9, 2014) – U.S. Marine Corps **Sergeant Justin T. Vogt** trains a fellow Marine as part of the Marine Corps Martial Arts Program at ISAF Headquarters in Kabul, Afghanistan. Vogt, who obtained his Black Belt in January 2012, has been a Marine Corps Martial Arts Instructor since September 2011. *Photo By: Lt. Michael J. Fallon*

Intelligence Oversight Division

MISSION: To ensure the effective implementation of Marine Corps-wide Oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Examples of sensitive activities include:

- Military support to Civil Authorities
- Lethal support/training to non-USMC agencies
- CONUS off-base training
- Covered, clandestine, undercover activities
- Intelligence collection of information on U.S. persons

SECNAVINST 5430.57G states:

"...personnel bearing USMC IG credentials marked 'Intelligence Oversight/Unlimited Special Access' are certified for access to information and spaces dealing with intelligence and sensitive activities, compartmented and special access programs, and other restricted access programs in which DON participates. When performing oversight of such programs pursuant to Executive Order, they shall be presumed to have a 'need to know' for access to information and spaces concerning them."

WHAT IS INTELLIGENCE OVERSIGHT?

Intelligence Oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories ([See References](#)).

DEFINITIONS

- INTELLIGENCE OVERSIGHT (IO):** Ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. References: E.O. 12333, DoD Dir 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3E, MCO 3800.2B
- SENSITIVE ACTIVITY OVERSIGHT:** Any activity requiring special protection from disclosure which could embarrass compromise or threaten the DON. Any activity which, if not properly executed or administered, could raise issues of unlawful conduct, government ethics, or unusual danger to DON personnel or property. These activities may include support to civilian law enforcement. Reference: [SECNAVINST 5000.34E](#)
- SPECIAL ACTIVITIES OVERSIGHT:** As defined by Executive Order 12333, activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies or media, and do not include diplomatic activities or the collection and production of intelligence or related support activities. Reference: [SECNAVINST 5000.34E](#)
- SPECIAL ACCESS PROGRAM (SAP):** Any Program imposing need-to-know or access controls beyond those normally required for Confidential, Secret or Top Secret information. Such a program includes but is not limited to a special clearance, more stringent adjudication or investigation requirements; special designation of officials authorized to determine need-to-know; or special lists of persons determined to have a need-to-know. A special access program may be a sensitive activity.
- QUESTIONABLE ACTIVITIES:** Any conduct that may constitute a violation of applicable law, treaty, regulation or policy.