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 9 Issue 1 Winter 2020

Photo by Sharon Bradford Franklin

IN THIS ISSUE, FEATURED ARTICLE: MODERN MASS SURVEILLANCE: IDENTIFY, CORRELATE, AND DISCRIMINATE

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

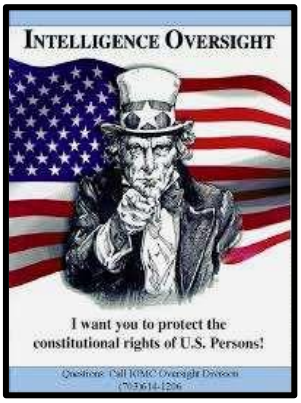
Mail:

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 Greg Stroh, Deputy Director
LtCol Greg Ryan, Sensitive Activities Officer

Inside This Issue



Web Links

Senior Intelligence Oversight Official (SIOO)
http://dodsioo.defense.gov/

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

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

A Message from the Director

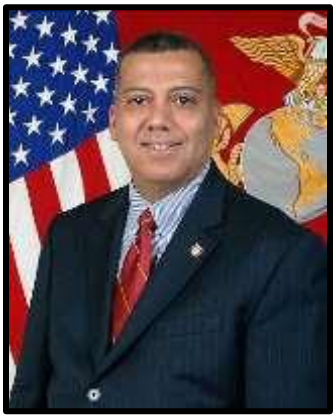
Greetings from the Office of the Inspector General for the Marine Corps, Oversight Division. This edition of *Overwatch* is the first of calendar year 2020. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Inspector General's Office. **There is new training available on MARINENET for intelligence oversight located at https://elearning.marinenet.usmc.mil/moodle/course/view.php?id=88. You must have a MARINENET account to participate. You may use this for your annual refresher training. Also, the new SECNAVINST 3820.3F, INTELLIGENCE OVERSIGHT WITHIN THE DEPT OF THE NAVY was published on 2 Jan 2020.**

The first article was written by Mr. Bruce Schneir who is an American cryptographer, computer security professional, privacy specialist and writer. He is a fellow at the Berkman Center for Internet & Society at Harvard Law School, and a program fellow at the New America Foundation's Open Technology Institute

The next article by Khalida Sarwari titled ***Map for artificial intelligence ethics oversight.*** *This article centers* on how to ensure that human values such as privacy and autonomy are protected as we adopt these systems.

Next, Ben Huebner, Chief of ODNI's Civil Liberties, Privacy, and Transparency Office discusses the Intel Community efforts to protect civil liberties when using Foreign Intelligence Surveillance Act (FISA) authorities.

Last, Sharon Bradford Franklin discusses the need for public engagement for robust intelligence oversight.



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

Featured Article

Modern Mass Surveillance: Identify, Correlate and Discriminate

By Bruce Schneier

www.schneier.com

January 2020

Communities across the United States are starting to ban facial recognition technologies. In May of last year, San Francisco banned facial recognition; the neighboring city of Oakland soon followed, as did Somerville and Brookline in Massachusetts (a statewide ban may follow). In December, San Diego suspended a facial recognition program in advance of a new statewide law, which declared it illegal, coming into effect. Forty major music festivals pledged not to use the technology, and activists are calling for a nationwide ban. Many Democratic presidential candidates support at least a partial ban on the technology.

These efforts are well-intentioned, but facial recognition bans are the wrong way to fight against modern surveillance. Focusing on one particular identification method misconstrues the nature of the surveillance society we're in the process of building. Ubiquitous mass surveillance is increasingly the norm. In countries like China, a surveillance infrastructure is being built by the government for social control. In countries like the United States, it's being built by corporations in order to influence our buying behavior, and is incidentally used by the government.

In all cases, modern mass surveillance has three broad components: identification, correlation and discrimination. Let's take them in turn.

Facial recognition is a technology that can be used to identify people without their knowledge or consent. It relies on the prevalence of cameras, which are becoming both more powerful and smaller, and machine learning technologies that can match the output of these cameras with images from a database of existing photos.

But that's just one identification technology among many. People can be identified at a distance by their heartbeat or by their gait, using a laser-based system. Cameras are so good that they can read fingerprints and iris patterns from meters away. And even without any of these technologies, we can always be identified because our smartphones broadcast unique numbers called MAC addresses. Other things identify us as well: our phone numbers, our credit card numbers, the license plates on our cars. China, for example, uses multiple identification technologies to support its surveillance state.

Once we are identified, the data about who we are and what we are doing can be correlated with other data collected at other times. This might be movement data, which can be used to "follow" us as we move throughout our day. It can be purchasing data, Internet browsing data, or data about who we talk to via email or text. It might be data about our income, ethnicity, lifestyle, profession and interests. There is an entire industry of data brokers who make a living analyzing and augmenting data about who we are -- using surveillance data collected by all sorts of companies and then sold without our knowledge or consent. There is a huge -- and almost entirely unregulated -- data broker industry in the United States that trades on our information. This is how large Internet companies like Google and Facebook make their money. It's not just that they know who we are, it's that they correlate what they know about us to create profiles about who we are and what our interests are. This is why many companies buy license plate data from states. It's also why companies like Google are buying health records, and part of the reason Google bought the company Fitbit, along with all of its data.

The whole purpose of this process is for companies -- and governments -- to treat individuals differently. We are shown different ads on the Internet and receive different offers for credit cards. Smart billboards display different advertisements based on who we are. In the future, we might be treated differently when we walk into a store, just as we currently are when we visit websites.

The point is that it doesn't matter which technology is used to identify people. That there currently is no comprehensive database of heartbeats or gaits doesn't

make the technologies that gather them any less effective. And most of the time, it doesn't matter if identification isn't tied to a real name. What's important is that we can be consistently identified over time. We might be completely anonymous in a system that uses unique cookies to track us as we browse the Internet, but the same process of correlation and discrimination still occurs. It's the same with faces; we can be tracked as we move around a store or shopping mall, even if that tracking isn't tied to a specific name. And that anonymity is fragile: If we ever order something online with a credit card, or purchase something with a credit card in a store, then suddenly our real names are attached to what was anonymous tracking information. Regulating this system means addressing all three steps of the process. A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible.

Similarly, we need rules about how our data can be combined with other data, and then bought and sold without our knowledge or consent. The data broker industry is almost entirely unregulated; there's only one law -- passed in Vermont in 2018 -- that requires data brokers to register and explain in broad terms what kind of data they collect. The large Internet surveillance companies like Facebook and Google collect dossiers on us are more detailed than those of any police state of the previous century. Reasonable laws would prevent the worst of their abuses.
Finally, we need better rules about when and how it is permissible for companies to discriminate. Discrimination based on protected characteristics like race and gender is already illegal, but those rules are ineffectual against the current technologies of surveillance and control. When people can be identified and their data correlated at a speed and scale previously unseen, we need new rules.

Today, facial recognition technologies are receiving the brunt of the tech backlash, but focusing on them misses the point. We need to have a serious conversation about all the technologies of identification, correlation and discrimination, and decide how much we as a society want to be spied on by governments and corporations -- and what sorts of influence we want them to have over our lives.

Map for artificial intelligence ethics oversight

by Khalida Sarwari
Northeastern University
August 29, 2019

With the introduction of new export controls on artificial intelligence software last week, the White House appealed to lawmakers, businesses, and European allies to avoid overregulation of artificial intelligence. It also maintained its refusal to participate in a project proposed by the Group of Seven leading economies, which seeks to establish shared principles and regulations on artificial intelligence, as the U.S. prepares to take over the presidency of the organization this year.
The U.S. has rejected working with other G-7 nations on the project, known as the Global Partnership on Artificial Intelligence, maintaining that the plan would be overly restrictive.

Kay Mathiesen is an associate professor of philosophy and religion in the College of Social Sciences and Humanities. Kay Mathiesen, an associate professor at Northeastern who focuses on information and computer ethics and justice, contends that the U.S.'s refusal to cooperate with other nations on a united plan could come back to hurt its residents.
Advocates of the plan say it would help government leaders remain apprised of the development of the technology. The project, they say, could also help build consensus among the international community on limiting certain uses of artificial intelligence, especially in cases where it's found to be controlling citizens or violating their privacy and autonomy.
U.S. leaders, including deputy chief technology officer Lynne Parker, counter that the proposal appears overly bureaucratic and could hinder the development of artificial intelligence at U.S. tech companies.
But Mathiesen says that many companies are already ahead of the curve in considering or implementing

oversight mechanisms to guide the ethical development of their products. She says that it's important to rein in the potentially harmful effects of artificial intelligence to ensure that the benefits of the technology are not overridden by the cost.

"The idea that we should just not regulate at all or not even think about this, because maybe then we might limit ourselves, I think that's a pretty simplistic view," says Mathiesen, a professor of philosophy who studies political philosophy and ethics. "It's not like the G-7 is going to have the power to all of a sudden impose regulations on U.S. industry. So that argument that merely by joining this [group] and beginning to think these things through, and do research on this, and develop [policy] recommendations—that that by itself is going to put us behind on artificial intelligence doesn't hold a lot of water."

Mathiesen suggests that failing to work with other countries in addressing privacy issues stemming from the unchecked spread of artificial intelligence products—such as facial recognition—could result in consumer backlash, and thereby slow down the development of artificial intelligence in the U.S.
"The technology is advancing incredibly rapidly and we want to make sure that we're thinking ahead, and we're building at the beginning protections for consumers before these things come out and it's too late and we have to try to fix problems that we could've prevented," she says.
The plan for the Global Partnership on Artificial Intelligence, which was introduced in December 2018, is to ensure that artificial intelligence projects are designed responsibly and transparently, in a way that prioritizes human values, such as privacy. The initiative received a major boost from Canada, which held the G-7's rotating presidency at the time, and was kept alive by France the following year. The U.S. will take over the presidency of the organization this year.
In addition to Canada and France, the other G-7 countries, including Germany, Italy, Japan, and the U.K., are on board with the project. The European Union, India, and New Zealand have also expressed interest. Mathiesen says that while she understands the concerns of some U.S. government officials about being out-competed, it's important for the U.S. to be a participating member in this effort, especially while the technology is still in its nascent stages.
'What do we want out of artificial intelligence? And, how do we get there?'

"In a way, it's better that the U.S. has buy-in at the beginning and is at the table to make these arguments about how do we balance concerns about things like privacy, security, and possible harm that could be produced by artificial intelligence? How do we balance that with also wanting to enable companies and inventors to create new things with artificial intelligence that can be economically and socially beneficial?" she says.

Mathiesen suggested that failing to engage in these conversations with the wider international community could leave the U.S. trailing behind.

"I think that the American citizens are going to suffer for that, just like they do now with the lack of data privacy," she says.

In conjunction with global professional services company Accenture, researchers at Northeastern' s Ethics Institute last year produced a report that provided organizations a framework for creating ethics committees to help guide the development of smart machines.

Civil Liberties, Privacy and Transparency Chief Speaks to Intelligence Oversight at Public Forum

Cato Institute
December 13, 2019

Ben Huebner, Chief of ODNI's Civil Liberties, Privacy, and Transparency Office, spoke about the Intelligence Community's (IC) efforts to protect civil liberties and privacy when using Foreign Intelligence Surveillance Act (FISA) authorities at the Cato Institute Surveillance Conference Dec. 6, in Washington, D.C.

The Cato Institute hosted the all-day public

conference to explore, independent of politics, the tension between holding intelligence agencies accountable to the legislative branch of government while allowing for the appropriate use of national security authorities.

Huebner joined privacy advocates as the only government participant on a panel entitled, "Overseeing Programmatic Surveillance: FISA §702 and §215."

Charlie Savage, Washington correspondent for the New York Times and the panel moderator, asked how the civil liberties oversight role differs at ODNI vice the CIA.

Huebner, who was previously the CIA's Privacy and Civil Liberties Oversight officer, said the role at CIA is more operational.

"Do we do programs or not?" said Huebner. "At ODNI, the role is more about determining the overall IC approach."

The panel discussed the IC's use of the USA FREEDOM Act that allows for the collection of call detail records (CDRs). In 2015, the USA FREEDOM Act made changes to Section 215 of the PATRIOT Act to include ending bulk collection by the government of domestic telephony metadata.

Said Huebner, the fundamental difference from the prior (Section 215) program is that under the USA FREEDOM Act, call detail records must now remain at the provider.

The USA FREEDOM Act provision authorizing CDRs was originally due to expire Dec. 15, until Congress extended its authorization three months as part of the short-term spending bill that kept the government funded. However, the government has stopped collecting CDRs.

When addressing whether Congress should reauthorize the CDR authority, Huebner explained that one point of view is, if "We're not using it, move on. But that doesn't mean it's not a useful tool in the toolkit. We want to use it when judiciously appropriate."

Savage also addressed the value of requiring national security authorities to expire through a sunset clause, explaining, "The notion of a sunset is periodic review (by Congress)."

The IC has to justify reauthorization, so that forces conversation about the value of those authorities, said Carrie Cordero, panelist from the Center for a New American Security.

"The goal of [the] USA FREEDOM [Act] was to put in more robust review and transparency," said Neema Singh Guliani, Legislative Counsel for the American Civil Liberties Union.

Guliani said the new program of collecting CDRs is better than the previous program, but still falls short of where we should be. She cited the positive creation of allowing for an amicus to be appointed to advocate before the FISA Court on novel and significant cases, but said the court sometimes rejects their arguments.

The panel then discussed oversight of FISA Section 702, which authorizes surveillance of non-U.S. persons reasonably believed to be outside the United States for foreign intelligence purposes.

"Oversight starts within the agencies," said Huebner. "But it's also a joint responsibility between the Department of Justice and my agency."

The FISC approves IC FISA 702 targeting, minimization and querying procedures that dictate how the government can obtain and use data.

Congress enacted FISA 702 with oversight by all three branches, executive, judicial and legislative.

"One issue," said Cordero, "is if that process still functions."

Other conference sessions included, "Watching the Detectives: Improving Intelligence Oversight;" "A Conversation with the Privacy and Civil Liberties Oversight Board;" and "Return of the Crypto Wars," among others.

The Cato Institute, according to its website, is a public

policy research organization — a think tank — dedicated to the principles of individual liberty, limited government, free markets, and peace. Its scholars and analysts conduct independent, nonpartisan research on a wide range of policy issues.

Public engagement is key for robust intelligence oversight

By Sharon Bradford Franklin
Policy Director at New America's Open Technology Institute (OTI).
January 29, 2020

***Discussion Prompt**: Is productive engagement on intelligence law, policy and oversight possible between the secret and civilian world and what can be gained from it? Reflections on best practice, lessons learned, and plans for the future*.

Bodies overseeing the activities of intelligence agencies often operate themselves in some necessary degree of secrecy. Despite this fact, or rather precisely because of it, regularly conferring with a dedicated civil society reference group is extremely valuable for both parties: it helps oversight bodies to not only diversify their views, but also to identify and address civil liberty risks, and it allows non-government actors to better understand declassified documents and have their voices heard.

In an earlier article on the engagement between civil society and the secret world of intelligence, Cheryl Gwyn, New Zealand's then Inspector-General of Intelligence & Security, described how she set up a civil society reference group to confer with her independent oversight agency, and explained how fostering openness and trust with civil society improved the performance of her agency.
Having worked both for an intelligence oversight body and for civil society organisations (CSOs) seeking reform of intelligence practices, I wholeheartedly agree with former Inspector-General Gwyn that engagement between the secret world of intelligence oversight and the civilian world of non-governmental organisations (NGOs) is not only possible, but is also worthwhile. Although it can be a frustrating process on both sides, I firmly believe that these two worlds can and should come together regularly to promote robust oversight and public accountability.

Worthwhile engagement

I served as Executive Director for the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) from the fall of 2013 through January 2017. This independent oversight body is tasked with reviewing U.S. counterterrorism programs to ensure that they comply with the law and include adequate safeguards for privacy and civil liberties. The PCLOB is headed by a bipartisan slate of five Board Members, and as Executive Director, I directed the work of our staff in supporting and carrying out the Board's mission. All Board Members and staff were required to have security clearances, and a critical part of our work involved reviewing classified information. But, like Inspector-General Gwyn — who sought outside perspectives to help ensure her agency's views were not "overly limited" by being contained "in the classified national security 'bubble'" — the PCLOB sought regular input from NGO advocates.
Having come from the NGO world, I reached out to a variety of civil society representatives and invited them to a series of sessions in which they could provide input to the PCLOB. Although Board Members were limited in the extent to which they could share their views with the NGO community, these sessions provided a valuable opportunity for the PCLOB to hear from advocates about what programs and issues they recommended for PCLOB review, and the privacy and civil liberties risks they felt these programs presented. In particular, it was helpful for the NGO representatives — who necessarily lacked access to classified information — to share their recommendations for the questions the PCLOB should ask of the intelligence agencies when conducting oversight reviews.

Civil society feedback

Following a session with a great many CSO representatives in December 2014, the PCLOB published a memo outlining the input received during its course. This session covered the PCLOB's review

of activities conducted under Executive Order 12333, which governs most of the U.S. intelligence community's operations. Civil society representatives presented suggested frameworks for the PCLOB's analysis, key privacy and civil liberties threats to examine, and critical questions that the PCLOB should ask during its review. From the perspective of PCLOB staff, this session and other more informal ones were extremely helpful in flagging issues and providing context for our reviews.

Both before and after serving at the PCLOB, I have held positions with different NGOs, where my work has included reviewing publicly available information about intelligence programs and seeking reforms to ensure robust safeguards for privacy and civil liberties. As part of this work, I have had the opportunity to participate in numerous meetings between civil society representatives and intelligence oversight officials. In particular, the Office of Civil Liberties, Privacy and Transparency of the Office of the Director of National Intelligence (ODNI) has convened periodic meetings held under the Chatham House Rule to foster dialogue and information sharing.

Decoding declassified documents

Frequently, this office will set up a discussion session in connection with ODNI's disclosure of newly declassified documents to provide context and answer questions from the NGO community. On other occasions, these sessions cover upcoming debates over renewal of a surveillance authority and provide NGO representatives with an opportunity to present arguments for needed reforms. More often than not, the officials will state that they need to "take back" our questions to determine what information they can provide in an unclassified environment. This can be frustrating, and the eventual answers can be less than satisfying. Nonetheless, I have found that these dialogues are still valuable. In particular, classified government documents are not generally written to be understandable to the public once declassified versions are released, so having direct conversations with officials who can help explain the documents is helpful.

Three models of engagement

The positive views on engagement that I developed through my personal experiences have been reinforced by an extensive series of interviews I conducted in support of a report that I wrote with Eric Kind. In our report, Strategies for Engagement between Civil Society and Intelligence Oversight Bodies, published in 2018, we analyzed the relationships between CSOs and oversight bodies in eight countries: Australia, Canada, France, Germany, the Netherlands, New Zealand, the United Kingdom, and the United States. We interviewed both civil society representatives and oversight officials, and based on our review, we outlined three models for productive engagement between bodies that conduct oversight of surveillance and CSOs: cooperation toward a shared goal, activating oversight, and promoting better understanding between civil society and oversight. For example, when CSOs provide research memoranda or key questions to guide an oversight review, this can assist an oversight body toward the shared goal of ensuring that intelligence activities are conducted in accordance with the rule of law. With regard to activating oversight, CSOs can be influential in providing the public support needed to ensure that governments establish oversight bodies whose missions include transparency to the public. And as for promoting better understanding between civil society and oversight, the sessions we held at the PCLOB as well as the conversations organized by the ODNI Office of Civil Liberties, Privacy and Transparency have all served this purpose.

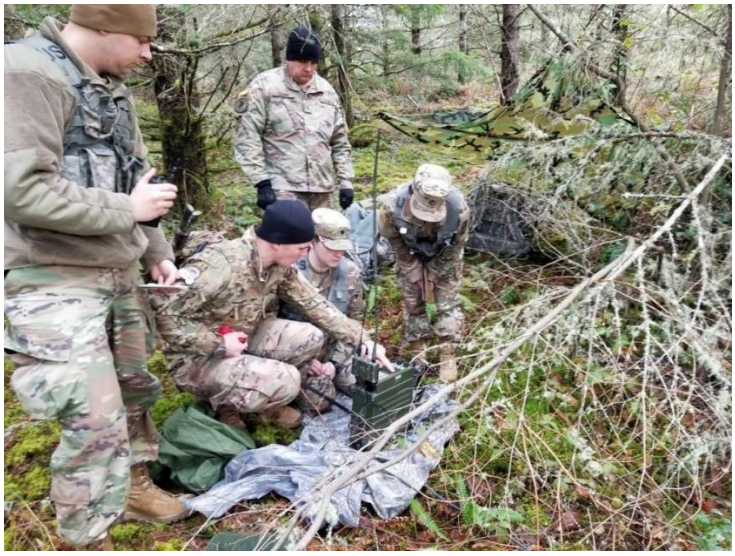
Possible steps forward

Our report includes a series of recommendations for increasing the amount, and improving the quality, of engagement between civil society and oversight going forward. These include urging oversight bodies to seek input from civil society on technological questions, noting that despite the barriers posed by classified information, outside technologists can nonetheless help ensure that oversight bodies are not relying solely on technical expertise from within the agencies they oversee. We also recommend several very practical steps, such as holding a series of offsite conferences to encourage sustained and frank dialogue.

Transparency renewed

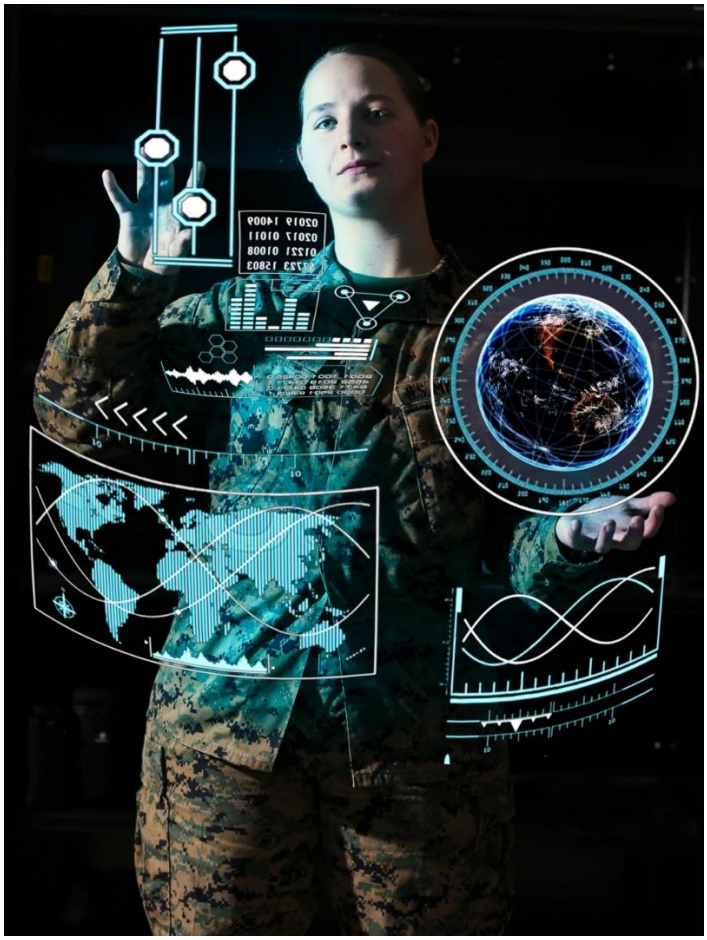
Shortly before I left my position at the PCLOB in January 2017, the agency lost a quorum of Board Members. Although it took almost two years, the PCLOB is now back up and running with a full slate of five Board Members. And in July 2019, the newly reinvigorated agency took an important step that Eric Kind and I had recommended: the PCLOB published a list of its current oversight projects. As we noted in our report, such transparency can promote public engagement and help CSOs to provide input to inform the oversight reviews. Hopefully, the PCLOB will also soon resume its practice of engaging directly with civil society representatives in addition to holding public hearings. I look forward to the opportunity to participate in these dialogues

Intelligence Photographs in the News



Soldiers from Delta Company 341st Military Intelligence Battalion conduct Low Level Voice Interception during the 341st Military Intelligence Battalion's field training exercise "Panther Strike Lite" on Feb. 8, 2020 at Joint Base Lewis-McChord, Wash. Panther Strike Lite was a battalion level exercise featuring Human Intelligence, Signal Intelligence and Counterintelligence in preparation for Panther Strike, a 300th Military Intelligence Brigade exercise at Camp Williams, Utah. (Courtesy Photo)

U.S. Marine Corps Pfc. Cara McClinton, an intelligence specialist with 2nd Intelligence Battalion, II MEF Information Group, poses for an environmental portrait as the unit's motivator of the week at Camp Lejeune, N.C. Dec. 18, 2019. According to her leadership, McClinton gives maximum effort and approaches problematic situations intelligently and methodically, always employing available resources to resolve issues. (This photo is an illustration; graphical elements were added to the image.) (U.S. Marine Corps Illustration by Sgt. David Delgadillo and Cpl. Peter Fillo.)



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

i. **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

ii. **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

iii. **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**

iv. **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.

v. **QUESTIONABLE ACTIVITIES:** Any conduct that may constitute a violation of applicable law, treaty, regulation or policy.