"Without Confirming or Denying": Opaque Notification and National Security Redress

Alex Joel

Executive Order (EO) 14086 establishes an innovative two-tier redress mechanism for individuals with "qualifying complaints" about U.S. signal intelligence activities. The European Commission (EC) has found that mechanism to meet European Union (EU) standards, and the European Data Protection Board (EDPB) is now working on its advisory opinion.

In this article, we focus on a specific aspect of the new redress mechanism: notification. EO 14086 requires that notification be provided "without confirming or denying that the complainant was subject to United States signals intelligence activities" (section 3(c)(i)(E)). In addition, the EO provides that the notification will state: "the review either did not identify any covered violations or the Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (ODNI) issued a determination requiring appropriate remediation."

This notification provision has generated controversy. On February 14, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (the LIBE Committee) published a draft resolution urging the EC not to adopt the draft adequacy decision. In its draft resolution, the LIBE Committee "points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data" (para. 5).

It is true that the redress process "is based on secrecy." As discussed below, what the draft resolution leaves out is the fact that national security redress processes *must* be "based on secrecy," otherwise they would be meaningless and ineffective. Investigators and adjudicators need access to classified information to carry out their responsibilities, and the results of their work will be classified as a result. This in turn will prevent them from "notify[ing] the complainant that their data has been processed" for so long as such notification would harm national security.

Given that this is a necessary aspect of providing effective redress, it should be no surprise that the legal norms in both the U.S. and the European Union (EU) allow for what this article refers to as "opaque notification." Indeed, the legal norm in the EU, as articulated by the Court of Justice for the European Union, is not that classified information must be disclosed to a complainant, but rather, that, as highlighted by the EDPB, "notification of persons whose data has been collected or analysed must occur only to the extent that and as soon as the notification no longer jeopardizes the tasks for which those authorities are responsible."

The Legal Norm of "Neither Confirm nor Deny"

In the U.S., Executive Order 13526 governs the classification, declassification, and handling of national security information. It provides that information may only be classified by "an original classification authority" who has determined that "unauthorized disclosure of the information reasonably could be expected to result in damage to the national security" (section 1.1(a)).

Importantly, the Order further provides that "[a]n agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors" (section 3.6). This is known in the U.S. legal system as the "Glomar response," named after the now-famous Glomar Explorer, a ship built by the CIA to secretly recover a sunken Soviet submarine during the Cold War. It is recognized by U.S. courts as a legally valid response when affirmance or denial would itself reveal classified information. One court put it this way: "[s]uch an agency response is known as a *Glomar* response and is proper if the fact of the existence or nonexistence of agency records falls within [the FOIA exemption for classified information]" (*Wolf v. C.I.A.*, 473 F.3d 370, 374 (D.C. Cir. 2007)).

As we further explore in a separate article, this is also the norm in Europe. The European Data Protection Board's (EDPB's) European Essential Guarantees for Surveillance Measures (EEG) highlighted the CJEU's finding in *La Quadrature du Net and others*, that "notification of persons whose data has been collected or analysed must occur only to the extent that and as soon as the notification no longer jeopardizes the tasks for which those authorities are responsible" (EEG para. 44). In addition, the EEG pointed out that the European Court of Human Rights "acknowledged that in some cases there might be no notification, however an effective remedy must be provided." Indeed, in a seminal case on surveillance Case of Klass and Others v. Germany (1978), the European Court of Human Rights (ECtHR) acknowledged:

> [T]he very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights (para. 55).

The Logic of "Neither Confirm nor Deny"

It may be helpful to explore why, as the ECtHR put it, "the very nature and logic of secret surveillance" prevents notification. Assume a complainant is under surveillance because intelligence agencies have reason to believe him to be a spy for a hostile foreign government. If the CLPO's review finds that there was an error in handling some of his data, a notification to that effect would alert him that his clandestine espionage activities had been detected, prompting him to take actions to avoid further surveillance. His intelligence service would immediately conduct a review to determine how his identity was compromised, undermining further signals intelligence efforts using those sources and methods. Clearly, then, such a notification would, as the CJEU put it, "jeopardize the tasks for which those authorities are responsible."

It may be less obvious how providing more information to other complainants could also expose sources and methods. Assume the government receives 100 complaints, only two of whom are under surveillance. If the government informs 98 complainants that they are not under

surveillance, and then tells two that the government can neither confirm nor deny anything related to the complaint, the government has in effect alerted those two that they are under surveillance.

This leads to the result we see in EO 14086 and in other such processes around the world: All complainants, not just those under surveillance, receive the identical initial response, one that neither confirms nor denies that the complainant was the subject of surveillance.

The Role of Notification: The CLPO Tier

Why, then, does the new EO even include a notification provision? If all notifications are identically and opaquely worded, what is the point? Simply this: the notification signals the end of important phases in the investigation and adjudication of the complaint, and triggers additional steps. Although the content of the notification is scripted, the outcome of the process that precedes it is not.

In the first tier of this process, the CLPO must conduct an investigation, make and document factual findings, determine whether a violation has occurred, and require mandatory remediation. It is clear from the EO that the CLPO will have access to classified information in order to carry out its responsibilities. Section 3(c)(i) of the EO directs that the CLPO's review be conducted "in a manner that protects classified information." The CLPO is to "review information necessary to investigate" the complaint and determine whether there was a covered violation. The CLPO must "provide a classified report" to the Foreign Intelligence Surveillance Court (FISC)--through the Department of Justice–if the CLPO finds information indicating a violation of any authority subject to FISC oversight. The CLPO must "maintain appropriate documentation" of the review and "produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation." It must then "prepare a classified ex parte record of review."

In addition, Section 3(c)(iii) directs each element of the Intelligence Community to "provide the CLPO with access to information necessary to conduct the reviews." This supplements the already-existing obligation in Executive Order 12333 for IC elements to ensure that privacy and civil liberties officers "have access to any information or intelligence necessary to perform their official duties" (section 1.6(h)). In addition, Intelligence Community Directive 126 provides further details on how the CLPO will carry out its responsibilities and directs IC elements to "provide [the CLPO with] access to information and personnel in a manner consistent with the protection of classified information or otherwise privileged or protected information."

What emerges from the above is that the CLPO–which has fully cleared staff, operates within sensitive compartmented information facilities, and uses secure computer and technology systems that are authorized to process and communicate classified information–must conduct an in-depth investigation of each qualifying complaint, with the full expectation that the investigation will focus on the classified information that is collected and processed by U.S.

signals intelligence activities. Indeed, without such complete access to classified information, it is difficult to see how a redress mechanism could hope to be effective. Naturally, the resulting mandatory record of the investigation, findings, and remediation (as applicable) will necessarily be classified and cannot be disclosed to the complainant.

It is after the CLPO completes this process that the notification is issued to the complainant. This now triggers the commencement of the second phase of the redress process. Under the EO, "the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General … apply for review of the CLPO's determinations by the Data Protection Review Court" (section 3(c)(i)(E)). Note that the EO contemplates that IC elements might be dissatisfied with the CLPO's findings—which are binding on them—and thus may themselves seek review from the DPRC. The regulation establishing the DPRC (28 C.F.R. Part 201) in turn provides that "[a] complainant may apply for review by the DPRC of a determination made by the ODNI CLPO . . . by filing an application for review with the appropriate public authority in a qualifying state . . . no later than sixty (60) days after the date … on which the complainant receives notification that the ODNI CLPO has completed its review" (Section 201.6).

The Role of Notification: The DPRC Tier

The application in turn kicks off the DPRC phase of the redress mechanism. The DPRC will convene a panel of three independent judges to review the complaint (section 201.8). In addition, a special advocate will be appointed to assist the panel by "advocating regarding the complainant's interest in the matter" and will have access to all information that is before the panel; in addition, the special advocate can submit questions and requests for information to the complainant through a process designed to ensure that no classified information is disclosed (section 201.8). The DPRC will determine whether a covered violation has occurred and if so the appropriate remediation; it will conduct its review based on the CLPO's record (which it can require be supplemented), and information and arguments submitted by the complainant, the special advocated and the IC (section 201.9). As with the CLPO, it is clear that the DPRC process, including the involvement of the Special Advocate will involve classified information. The regulation provides that both the DPRC judges and the special advocate must hold "requisite security clearances to access classified national security information" (section 201.11).

After the DPRC completes its review, it issues a final, binding written decision (section 201.9(g)). The complainant then receives a notification that states: "The review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation." As set forth in the regulation, "[t]he notification to the complainant constitutes the final agency action in the matter." The term "final agency action" is a legal term of art under U.S. law. As discussed in detail in Judicial Review of the Determinations of the New Data Protection Review Court Under the Administrative Procedure Act, we believe that the DPRC's rulings, as final agency actions, may well be subject to judicial

review under the Administrative Procedure Act. If so, the DPRC's notification of "final agency action" serves to trigger such review.

Declassification and Release

The fact that the record pertaining to a complaint is classified when prepared is not the end of the story. EO 14086 expressly contemplates that the record may be declassified, and if so, directs that the complainant be so notified:

> The Secretary of Commerce shall . . . not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint [by the CLPO and the DPRC] has been declassified . . . and … If informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint . . . may be available under applicable law (section 3(d)(v)).

As we explained in Redress: What is the problem?, once notified of surveillance an individual can establish "standing" and bring a case in federal district court.

How might such information be declassified? In the U.S., classification is governed by Executive Order 13526, Classified National Security Information. The Order establishes a complex set of controls governing how information is classified, protected, and shared, and how it must eventually be declassified. Importantly, EO 13526 prominently provides that "in no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security" (section 1.7). The Order makes clear that "[n]o information may remain classified indefinitely" (section 1.5(d)). It elaborates on this rule, specifying that "[i]nformation shall be declassified as soon as it no longer meets the standards for classification under this order," in which case it is to be declassified by the original classification authority or by the DNI (section 3.1).

The Order lays out a range of formal avenues for declassification. We will focus on two for these purposes. First, even if information continues to meet classification standards, the appropriate authority may choose to declassify information in the public interest:

> It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, [the responsible official] will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure (section 3.1(d)).

The DNI has used this authority to declassify certain documents now posted on IC on the Record. For example, DNI James Clapper declassified a range of documents in 2013, stating:

> Over the past months, I've declassified and publicly released a series of documents related to both Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, or FISA. We're doing that to facilitate informed public debate about the important intelligence collection programs that operate under these authorities. We felt that in light of the unauthorized disclosures, the public interest in these documents far outweighed the potential additional damage to national security.

Second, EO 13526 provides that persons can seek information and documents from federal agencies through a "mandatory declassification review" (MDR) request. EO 13526 directs agencies conducting a mandatory review to "declassify information that no longer meets the standards for classification under this order" (section 3.5(c)). Requestors who are not satisfied with an agency declassification determination may appeal it to the Interagency Security Classification Appeals Panel (ISCAP) (section 3.5(f), section 5.3).

The request must "describe the document . . . with sufficient specificity to enable the agency to locate it with a reasonable amount of effort" (section 3.5(a)(1)); given the meticulous documentation for each complaint that EO 14086 requires, this poses no hurdle. In addition, the information cannot be an "operational file" that is exempted from search or review in connection with Freedom of Information Act requests. While the record here might refer to such information, it is unlikely that the record of review created by the CLPO and the DPRC—which are oversight bodies and are not "operational" in nature—would be deemed an "operational file."

A more difficult hurdle lies in Section 3.5(h), which in essence limits the MDR avenue to U.S. persons. That said, a U.S. person (including, for example, a U.S. privacy or open government advocacy organization) could initiate the MDR process for these records, so long as they are not acting directly on behalf of a foreign government or individual. Indeed, we believe a U.S. government entity could initiate an MDR request relating to these records, such as the CLPO, the PCLOB, the DPRC or the Secretary of Commerce (section 1.8 referred to below is another avenue for government officials).

In addition to the above two declassification avenues, EO 13526 provides for internal challenges to classification decisions. It specifies that "[a]uthorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information." Agencies must ensure that challenges "are not subject to retribution for bringing such actions," that the challenge will be reviewed "by an impartial official or panel" and that decisions can be appealed to the ISCAP (section 1.8). Given that both the CLPO and the DPRC are "authorized holders of information," they are well-positioned to challenge classification decisions that they believe to be improper.

Note that declassification does not necessarily equate with publication. That is, once declassified, a record would still be protected from public disclosure to preserve privacy. The record could, however, no longer be exempt from disclosure for national security reasons to an individual requestor under the Freedom of Information Act (FOIA). There is no U.S. person limitation under FOIA; any individual, regardless of nationality, can submit a request. Thus, once notified of declassification, a complainant under EO 14086 could submit a FOIA request for their records.

What about the ISCAP—is it an effective appellate body? Open government advocates have praised this panel for being willing to overturn agency decisions. According to one noted advocate, this panel

> has frequently ruled in favor of requesters and against the positions of its own member agencies. . . . [It] has declassified all or some information in a clear majority of the disputed cases it reviewed, even though the classifying agency had refused to do so. This phenomenal record deserves more consideration than it has received to date (pp. 525-526).

Going forward, t may be helpful to publish more specific guidance on declassification reviews of these redress records. The DNI could, for example, issue an Intelligence Community Standard under ICD 126 to establish a process for periodic declassification review of the CLPO and DPRC final redress records. This would regularize the process and provide further assurance that such records will be declassified once disclosure will no longer harm national security.

Other Avenues for Transparency

Additional avenues are available under current law for transparency regarding certain aspects of the redress process. For example, the CLPO is already obligated under existing law to publish a semiannual report that documents, among other things, "the number and nature of the complaints received . . . for alleged violations; and a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer" (42 U.S.C. section 2000ee-1). The CLPO posts these reports on its website (see, e.g., the July 2022 report). Going forward, the CLPO will need to include in this report a description of the complaints it investigates under the EO 14086 process.

In reporting on those complaints, the CLPO is guided by the Principles of Intelligence Transparency for the IC. Those principles establish the overarching framework for proactive transparency for intelligence agencies. Among other things, the principles call on the IC to "[p]rovide appropriate transparency to enhance public understanding about . . . the laws, directives, authorities and policies that govern the IC's activities" as well as "the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules." The principles have been baked into the IC's governance framework. For example, Intelligence Community Directive 107, Civil Liberties, Privacy, and Transparency, states: "To provide greater public transparency without causing damage to national security, IC

elements shall . . . [s]upport robust implementation of the Principles of Intelligence Transparency for the IC" (section D.3). In addition, the principles are officially part of the National Intelligence Strategy, which calls on the IC to "practice appropriate transparency to enhance accountability and public trust (Enterprise Objective 7). Thus, in meeting its reporting obligations as well as in carrying out its efforts to enhance transparency, it can, consistent with the principles, seek to provide information relating to the "laws, authorities, directives, and policies" that are being applied in determining whether violations have occurred.

Another avenue for transparency on these matters is the Privacy and Civil Liberties Oversight Board (PCLOB), which is to conduct an annual review of the redress process, "including whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner; whether the CLPO and the Data Protection Review Court are obtaining full access to necessary information; whether the CLPO and the Data Protection Review Court are operating consistent with this order; whether the safeguards established by section 2 of this order are properly considered in the processes of the CLPO and the Data Protection Review Court; and whether the elements of the Intelligence Community have fully complied with determinations made by the CLPO and the Data Protection Review Court" (section 3(e)). The PCLOB is to "release to the public an unclassified version of the report" and will "make an annual public certification as to whether the redress mechanism . . . is processing complaints consistent with this order" (section 3(e)(iii)).

The PCLOB does not hesitate to push the IC to declassify information so that the PCLOB's reports can better inform the public. For example, as part of its seminal report on FISA Section 702, the Privacy and Civil Liberties Oversight Board stated:

> [T]he Board requested declassification of additional facts for use in this Report. . . . The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process, and as a result of the process, many facts that were previously classified are now available to the public. (P. 3)

An additional avenue is the requirement for the Department of Justice and the Office of the Director of National Intelligence to prepare a joint report documenting their assessment of the IC's compliance with Section 702 of the Foreign Intelligence Surveillance Act (50 U.S.C. § 1881a(m)(1))). There is no congressional mandate for these highly detailed and classified reports to be redacted and publicly released, yet the ODNI has been doing so for many years. The most recent report is posted here. EO 14086 provides that if, as part of the redress mechanism, the CLPO or the DPRC identify FISA violations, they must report those to the Foreign Intelligence Surveillance Court (via the Department of Justice) (sections 3(c)(1)(d) and 3(d)(1)(f)). If those violations involve FISA Section 702, they would form part of the semiannual joint assessments.

These avenues could well result in transparency that could not only inform the public, but also complainants about how the redress mechanism is interpreting and applying applicable laws—including EO 14086—in adjudicating complaints. There is precedent for such transparency. Even before Congress mandated a review (with an eye toward release) of classified opinions of the Foreign Intelligence Surveillance Court that presented significant constructions or interpretations of law, the ODNI had announced its own review for release of such opinions. The ODNI recently announced that all remaining FISC decisions that include a significant construction of law have now been released.

Conclusion

The records of review by the CLPO and the DPRC are classified when prepared and issued. This reflects the fact that they have full access to classified information in executing their responsibilities and is in keeping with existing legal norms for protecting information that could harm national security. The notification signals the completion of important phases of the redress process and can trigger additional actions for the complainant, such as requesting DPRC review and, possibly, initiating judicial review under the Administrative Procedure Act.

The records may only remain classified for so long as disclosure would cause damage to national security. Agencies must declassify records that no longer meet classification standards, and in addition can declassify information if the public interest outweighs the harm to national security that release could cause. Moreover, a declassification review must take place pursuant to an MDR request or a classification challenge, with appeal. EO 14086 contemplates that such records may be declassified and requires the Secretary of Commerce to check periodically the classification status of records, and if declassified, to so notify the complainants (via the appropriate public authority).

In short, notification can occur once doing so "no longer jeopardizes the tasks for which those authorities are responsible." The standard for notification under U.S. law is therefore effectively the same as that under EU law.

The author served for 14 years as the CLPO for the ODNI, and recounted what he learned about the national security legal framework in Protecting Privacy and Promoting Transparency in a Time of Change: My Perspective after 14 Years as Civil Liberties Protection Officer. The author thanks Francesca Oliveira and Lauren Mantel for their research assistance in the preparation of this paper.

The views expressed in this publication are the author's and do not imply endorsement by the Office of the Director of National Intelligence, the Intelligence Community, or any other U.S. Government agency.