

ANALYSIS

How the FBI Violated the Privacy Rights of Tens of Thousands of Americans

A recently released secret court ruling found that the government's warrantless surveillance of emails routinely violated the Fourth Amendment.



Elizabeth Goitein

October 22, 2019

This article was originally published by Just Security in [two](#) [\[link-1\]](#) [parts](#) [\[link-2\]](#).

Earlier this month, the Office of the Director of National Intelligence released three redacted opinions of the Foreign Intelligence Surveillance Court (also known as the FISA Court) and the FISA Court of Review (FISCR). In the [first opinion](#) [\[link-3\]](#), the FISA Court held that the FBI's procedures for accessing Americans' communications that are "incidentally" collected under Section 702 of FISA violated both the statute and the

Fourth Amendment. The government appealed, and in the [second opinion](#) [\[link-4\]](#), the FISCR upheld the FISA Court's decision. The FBI was forced to revise its procedures to conform with the court's ruling, and in the [third opinion](#) [\[link-5\]](#), the court approved the revised procedures.

The government will no doubt try to sell this as an oversight success story. After all, the Department of Justice's audits had detected instances of FBI non-compliance with legal requirements, and the Department reported those instances to

the FISA Court. The court solicited the assistance of *amici* and adopted their position in significant part. It ordered remedies that the FBI is now required to implement. And all of this became public because Congress in 2015 required the disclosure of significant FISA Court opinions. The system worked, right?

I see a very different story. This is now the fourth major FISA Court opinion on Section 702 in 10 years documenting substantial non-compliance with the rules meant to protect Americans' privacy. The opinion, moreover, reveals that the FBI is conducting literally *millions* of backdoor searches — including so-called “batch queries” that rest on the same discredited legal theory used to justify the NSA's bulk collection of Americans' phone records. Despite the enormous implications for Americans' privacy and the government's dismal record, the remedy suggested by *amici* and imposed by the court was just more record-keeping. And the government sat on the opinion for a year, hoping

for an appellate victory that would help mitigate the PR damage from disclosure.

Background: Section 702's Troubled History

To put the court's recent opinions in context, some background is necessary. Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), passed in 2008, the National Security Agency (NSA), operating inside the United States, is authorized to collect communications of foreigners overseas for foreign intelligence purposes. No warrant is required for this collection because courts have held that foreigners have no Fourth Amendment rights. Instead, each year, the FISA Court must sign off on the procedures that govern the surveillance.

Although ostensibly targeted at foreigners, Section 702 surveillance inevitably sweeps in massive amounts of Americans' communications. Recognizing the impact on Americans' privacy, Congress required the NSA to “minimize” the sharing, retention, and use of this “incidentally” collected U.S. person data. But the government and the FISA Court have embraced an interpretation of “minimize” that is remarkably... maximal. The NSA shares raw

data with multiple other agencies — including the FBI and the CIA — and all of them retain the data for a functional minimum of five years. Moreover, the FBI routinely combs through it looking for Americans' communications to use in purely domestic cases, even in situations where the FBI lacks a factual predicate to open a full investigation.

In 2011, the government disclosed to the FISA Court that it had misrepresented the nature of its “upstream” collection activities under Section 702. (“Upstream” collection takes place as the communications are transiting over the Internet backbone; “downstream” collection acquires stored communications, usually from the servers of Internet Service Providers.) When conducting upstream surveillance, the government was acquiring, not just communications *to or from* the targets of surveillance, but communications that simply mentioned certain information *about* them (known as “abouts” collection). As a result, the government was acquiring packets of data containing multiple communications, some of which had nothing to do with the target. This included tens of thousands of wholly domestic communications.

The court was not pleased to learn about this significant issue three years into the program's operation. **It held** [\[link-6\]](#) that

the government's handling of the data violated the Fourth Amendment, and it required the government to develop special rules — approved by the court in 2012 — for segregating, storing, retaining, and accessing communications obtained through “upstream” collection.

In 2015, the court was under the impression that these rules were being followed. However, in approving Section 702 surveillance that year, **it noted** [\[link-7\]](#) several incidents of non-compliance with *other* rules designed to protect Americans' privacy — including FBI violations of protections for attorney-client communications, a “failure of access controls” by the FBI, and the NSA's failure to purge certain improperly collected data. Once again, the court expressed displeasure at being notified of infractions long after they occurred.

In 2016, the **FISA Court learned** [\[link-8\]](#) that the NSA had been violating the rules established in 2012. Because those rules were designed to remedy a Fourth Amendment violation occurring since the start of the program, the NSA's non-compliance meant that its upstream collection activities had been operating unconstitutionally for eight years. Moreover, the government did not report this issue for several months after discovering it. Unable to bring itself into compliance, the NSA made the only decision it could: In the spring of

2017, it abandoned “abouts” collection, which was at the root of the problem.

When Section 702 came up for reauthorization in late 2017, civil liberties advocates pointed to this troubled history. They also pointed to a growing body of case law holding that searches of government databases can, in certain circumstances, constitute a separate Fourth Amendment event. They argued that government agencies should be required to obtain a warrant before searching Section 702-obtained data for the communications of Americans (a practice formally called “U.S. person queries” and informally dubbed “backdoor searches”). They also urged Congress to ban “abouts” collection, lest the government attempt to resume it.

Congress **rejected these proposals** [\[link-9\]](#). Although Congress did require the FBI to obtain the FISA Court’s permission to conduct U.S. person queries in a tiny sliver of cases, it blessed the vast majority of these searches, which previously had no foundation in the text of Section 702. It simply required the FBI to develop “querying procedures” that the FISA Court would have to approve. It also required the FBI to keep records of each U.S. person query it conducted. With respect to “abouts” collection, Congress required the government to obtain FISA Court approval and to give

Congress advance notice before resuming the practice.

The court’s October 2018 Ruling

In March 2018, the government submitted its annual certifications and procedures to the FISA Court for its approval. In a decision dated October 18, 2018, and released last week, the FISA Court held that the FBI’s minimization procedures violated both the statute and the Fourth Amendment. The court’s opinion addresses three main practices by the FBI: downstream collection of certain communications; the FBI’s failure to record USP queries; and the FBI’s improper use of USP queries.

Downstream collection and “abouts” communications. Although this section of the opinion is highly redacted, it appears that the government is engaged in a new form of downstream collection that raised a flag for the FISA Court. The court solicited *amici*’s advice about whether the statutory preconditions for resuming “abouts” collection apply to downstream collection, and whether certain activities in the government’s 2018 certifications involve the acquisition of “abouts” communications. *Amici* argued that the answer to both questions was yes; the

government's answer was no in both cases. The court split the baby, holding that the statutory requirements apply to any kind of "abouts" collection, but that no such collection would occur under the government's certifications.

The heavy redactions make it difficult to assess the significance of this part of the opinion. However, on its face, the definition of "abouts" collection — basically, anything other than a communication *to* or *from* the target — should not be difficult to apply. It is worrisome that the government and *amici* reached different conclusions about whether a certain form of collection merited the label "abouts." The uncertainty strongly supports a suspicion civil liberties advocates have held for some time: that the selectors the government uses to identify the communications to be collected are not necessarily unique identifiers (such as email addresses), but can sweep in people other than the intended targets (as would, for instance, IP addresses).

The statutory requirement to count U.S. person queries. In its January 2018 reauthorization of Section 702, Congress ordered the government to adopt querying procedures that included "a technical procedure whereby a record is kept of each United States person query term used for

a query." Instead, in the querying procedures that the FBI submitted to the FISA Court, the Bureau announced that it "intends to satisfy the record-keeping requirement by keeping a record of all queries" — in other words, the FBI would lump together U.S. person queries and non-U.S. person queries, without distinguishing between them.

The government defended this approach with a weak argument that the statutory text was somehow ambiguous, and that both the legislative history and policy considerations weighed against requiring the FBI to document U.S. person queries. In a refrain often heard when an intelligence or law enforcement agency is asked to devote time or resources to safeguarding civil liberties, the government claimed that requiring the FBI to figure out whether a particular investigative subject was a U.S. person would "divert resources from investigative work . . . to the detriment of public safety."

The FISA Court has historically yielded to such pleas, and on this occasion, the court seemed sympathetic. Ultimately, however, the court concluded that it had no choice. It stated: "Regardless of how persuasive the FBI's considerations may be, the court is not free to substitute its understanding of sound policy — or, for that matter, the understanding of the Director of the FBI —

for the clear command of the statute.” The law, the court held, was unambiguous in its directive to count U.S. person queries.

On appeal, the FISCER upheld the court’s ruling on this question. The FISCER, however, seemed somewhat less sympathetic to the government’s position. Under the FBI’s querying procedures, “U.S. person query term” is defined as “a term that is reasonably likely to identify one or more specific United States persons.” This definition does not require a high level of certainty. Moreover, the procedures provide for the application of default assumptions in cases where specific information is lacking. Under these circumstances, it is hard to argue with the FISCER’s assessment that counting U.S. person queries is not “a burdensome substantive requirement,” and that it would simply mean “adding one (largely ministerial) item to the checklist that FBI personnel most likely already work through when conducting queries for investigative purposes.”

Somewhat oddly, the FISCER did not resolve the other major issue on appeal: whether the FBI’s repeated violations of its own querying and minimization procedures rendered those rules unlawful and unconstitutional as implemented. Those violations, and the FISA Court’s failure to require an adequate remedy for them, will be the subject of Part II of this post.

Improper queries of Section 702 communications. The most eye-opening part of the October 2018 opinion is the section addressing the “large number” of queries undertaken by the FBI since April 2017 that did not comply with internal rules, the statute, or the Fourth Amendment.

To begin, the opinion provides the first glimpse of just how prevalent the FBI’s U.S. person queries really are. In the past, the FBI has claimed it has no way even to estimate this number. It was nonetheless clear that the number was significant, as the Privacy and Civil Liberties Oversight Board (PCLOB) **reported** [\[link-10\]](#) that the FBI runs queries of databases containing Section 702 data at the earliest stage of every assessment or investigation.

The court’s October 2018 opinion reveals that the FBI in 2017 conducted 3.1 million queries *on one system alone*. This number encompasses U.S. person and non-U.S. person queries alike, but as the court observed: “[G]iven the FBI’s domestic focus it seems likely that a significant percentage of its queries involve U.S.-person query terms.” Almost certainly, then, the total number of U.S. person queries run by the FBI each year is well into the millions.

In theory, the FBI’s procedures are supposed to limit these searches. The key limitation, as set forth in the querying procedures, is as follows:

“Each query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures.”

This requirement essentially mirrors the one previously contained in the FBI’s minimization procedures. The FISA Court once again held, as it has in the past, that this limitation, “as written,” satisfies both the statute and the Fourth Amendment.

But that didn’t end the court’s analysis. The court went on: “FISC review of minimization procedures under Section 702 is not confined to the procedures as written; rather, the court also examines how the procedures have been and will be implemented.” The court then noted that, “[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime.” These included multiple one-off incidents of FBI personnel running U.S. person queries accidentally or for improper personal purposes. (In a frank statement that reveals why limits on access are a poor substitute for adequate limits on collection, the FISA Court commented that it was less concerned about personal misuses of the data, because “[i]t would be difficult to completely pre-

vent personnel from querying data for personal reasons.”) They also included several incidents indicative of more systemic problems, including:

- In March 2017, the FBI, against the advice of the FBI’s Office of General Counsel, conducted queries using 70,000 identifiers “associated with” people who had access to FBI facilities and systems.
- On a single day in December 2017, the FBI conducted over 6,800 U.S. person queries using Social Security Numbers.
- Between December 7–11, 2017, an FBI official improperly reviewed raw FISA information resulting from 1,600 U.S. person queries.
- On more than one occasion, the FBI conducted dozens of U.S. person queries to gather information about potential informants.

The government told the FISA Court that these errors stemmed from “fundamental misunderstandings by some FBI personnel [about] what the standard ‘reasonably likely to return foreign intelligence information’ means.” This is a remarkable admission, given that this standard has been in place for several years, and given the government’s repeated assurances to the FISA Court during this time that access to Americans’ data was restricted to person-

nel who were carefully trained in the applicable limits.

The court expressed “serious concern” about “the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it.” It identified three factors that heightened its concern. First, it cited limitations on existing oversight mechanisms. It noted that some FBI offices field offices go for periods of two years or more between oversight visits, and ultimately, Justice Department overseers “review only a small portion of the queries conducted.” It also observed that “the documentation available to [overseers] lacks basic information that would assist in identifying problematic queries.” Given these limitations, the court wrote, “it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the court.”

Second, the court — for the first time — acknowledged the tension between the substantive limits on queries contained in the FBI’s procedures, and the Bureau’s vigorous encouragement to its personnel to run queries early and often. Indeed, an FBI official submitted a declaration to the court stating that “FBI encourages its personnel to make maximal use of queries — provided they are compliant with the FBI’s

minimization procedures” FBI officials are thus simultaneously told to *maximize* and *minimize* their access to U.S. person information. In the court’s words:

“On the one hand, the FBI is obligated to query Section 702 and other FISA information only in circumstances satisfying a querying standard that does not apply to FBI information generally. On the other hand, it has set up its systems to facilitate running the same query simultaneously across FISA and non-FISA datasets . . . and encourages personnel to make maximal use of such queries, even at the earliest investigative stages. Those policy decisions may well help FBI personnel work efficiently and ‘connect dots’ to protect national security . . . but they also create an environment in which unduly lax applications of the Section 702 querying standards are more likely to occur.”

Third, the court discussed the FBI’s use of “batch queries” — perhaps the most explosive revelation in the opinion. The FBI’s querying procedures require that “[e]ach query” must be reasonably likely to retrieve foreign intelligence information or evidence of a crime. The government, however, has taken the position that “an aggregation of individual queries” — also referred to as a “batch query” — “can satisfy the querying standard, even if each in-

dividual query in isolation would not be reasonably likely to return foreign-intelligence information or evidence of a crime.” So, for instance, if the FBI has information that an employee at a particular company is planning illegal actions, but the FBI has no knowledge of who the employee is, the Bureau would be justified (the government argues) in running queries for *every employee at that company*. This is presumably the theory on which the FBI ran the massive numbers of queries described above (e.g., 70,000 queries on individuals with access to FBI systems and facilities).

If this sounds familiar, it should. This is the same rationale the NSA used to justify “bulk collection” of Americans’ telephone records. Even though the applicable statute, Section 215 of the Patriot Act, allowed the government to obtain records only if they were “relevant” to an authorized investigation, the FISA Court allowed the NSA to collect the phone records of nearly every American — most of which were, of course, entirely irrelevant to any investigation — on the ground that some relevant records were likely buried within them. When this practice was made public as a result of Edward Snowden’s disclosures, it was unable to withstand either judicial review (the Second Circuit Court of Appeals held that it violated the statute) or the judgment of Congress (which

changed the law in 2015 with the goal of prohibiting bulk collection).

As the NSA’s bulk collection program illustrates, there is no logical limit to how many queries the FBI could aggregate based on the theory that the result will likely yield foreign intelligence or evidence of a crime. Indeed, the larger the number of individuals swept in, the more likely it is that the queries, in aggregate, will turn up results. It is a small step from “batch queries” to “bulk queries.” The court did not seem alarmed by the implications of the theory — it opined that “[p]erhaps in the abstract it would be reasonable for the FBI to run such an aggregated query” — but it nonetheless expressed skepticism that such an approach could be reconciled with the text of the FBI’s querying procedures, which require “[e]ach query” to be reasonably likely to return foreign intelligence information or evidence of a crime.

Ultimately, the court held that the extent of improper querying rendered the FBI’s procedures, as implemented, inconsistent with Section 702’s “minimization” requirement. It also held that the FBI’s practices violated the Fourth Amendment’s reasonableness requirement. Although it found the government’s interest in acquiring foreign intelligence information to be “particularly intense,” it quoted a decision by the *Foreign Intelligence Surveillance Court*

of Review (FISCR) stating that if “the protections that are in place for individual privacy interests are . . . insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.” The court concluded: “Here, there are demonstrated risks of serious error and abuse, and the court has found the government’s procedures do not sufficiently guard against that risk.”

To cure these defects, the court recommended — and the FBI ultimately adopted, after the government’s unsuccessful appeal to the FISCR — a remedy proposed by *amici*. Specifically, any time the FBI runs a U.S. person query that returns Section 702 data, FBI personnel are not permitted to view the content (although they may still view non-content “metadata”) unless they first document the reasons why they believed the query was likely to return foreign intelligence or evidence of a crime. The court opined that this requirement would force FBI personnel to think more carefully about the applicable standard before running queries, and would assist oversight personnel in

determining whether the standard was indeed being honored.

A Triumph of Oversight?

The FISA Court identified serious problems with the government’s submissions, engaged *amici* to provide advice, considered and partly agreed with their arguments, held the government’s actions to be not only unlawful but unconstitutional, and adopted a remedy proposed by *amici* — all of which was made public, albeit with redactions. Taken in isolation, these facts might seem to tell a resounding success story for oversight of foreign intelligence surveillance.

But such a conclusion would ignore many other salient facts. For one thing, the government sat on the FISA Court’s October 2018 opinion for almost a year, instead of promptly declassifying and releasing it as envisioned by Congress in the 2015 USA FREEDOM Act. Clearly, the government was hoping for a win on appeal that would neutralize the negative impact on public opinion. Had the appeal taken several additional months to resolve, there is no doubt that we would still be in the dark about the FBI’s activities today.

As for the substance of the opinion, the illusion of accountability fades when one

considers the many aspects of the court's own ruling that were left entirely undressed by its chosen remedy. The court's opinion cited the following major problems and sources of concern:

- FBI personnel are fundamentally confused about what “reasonably likely to return foreign intelligence or evidence of a crime” means.
- Oversight is limited because overseers review only a tiny fraction of queries.
- Oversight is limited because overseers lack documentation of the justification for queries.
- There is a mismatch between the FBI's querying procedures, which purport to place substantive limits on queries, and the FBI's policy of encouraging routine use of those queries at the earliest stage of every investigation.
- “Batch” queries are seemingly inconsistent with the text of the FBI's querying procedures.

The remedy imposed by the court — a requirement that FBI personnel document their reasons for performing a U.S. person query before viewing content information — addresses only one of these problems (lack of documentation for overseers to review). After all, if FBI agents truly do not understand what “reasonably likely to return foreign intelligence or evidence of a crime” means, requiring them to docu-

ment their misconceptions will not produce any greater understanding; it will merely reaffirm the confusion that the court already observed.

In theory, the documentation could be used as a mechanism to identify personnel who require remedial training or even administrative discipline. But the court did not order any such measures, and the FBI's revised procedures don't contemplate them. In any case, it is clear from the court's opinion that the Justice Department would require expanded oversight capacity to detect non-compliance in anything more than a fraction of cases. The court did not direct the Justice Department to devote more resources to oversight, and so virtual piles of documentation recording FBI agents' various interpretations of the legal standard for queries will languish unexamined. Knowing this, FBI agents are unlikely to spend much time or thought on writing out their rationales.

Nor does the court's remedy do anything about the mixed message the FBI sends its personnel by simultaneously limiting (in its querying and minimization procedures) and urging (in its policies and rhetoric) the use of queries. It was an important step forward for the court to recognize this fundamental disconnect in the FBI's practice. But the disconnect will con-

tinue unless and until the court orders the FBI to harmonize its policies and its rhetoric with its Section 702 procedures.

The court also strongly suggested that “batch queries” are inconsistent with the text of the FBI’s querying procedures. However, it did not order the FBI either to stop batch queries or to alter its procedures to allow them. The FBI’s revised procedures, which the FISA Court approved in September 2019, still have the language that would seem to foreclose batch queries. But there is no indication, either in the procedures or in any other public document, that the FBI has stopped the practice; and the FISA Court apparently forgot to ask, as its September 2019 opinion does not even mention the issue.

More to the point, the court should have barred “batch queries” outright. The FISA Court’s finding that Section 702 surveillance is constitutionally reasonable has always hinged on a delicate balance between the government’s interest in collecting foreign intelligence and Americans’ privacy interests in their communications. The ostensible existence of strict limitations on government officials’ access to Americans’ communications — including the requirement that queries must be designed to return foreign intelligence or evidence of a crime — has been a key factor in the court’s conclusion that the balance

tips in the government’s favor. Allowing the FBI to conduct tens of thousands of queries in a “batch,” when it is apparent that the vast majority of them will *not* yield any such information or evidence, would require a significant repositioning of the scales.

One final observation: The court’s modest record-keeping remedy is particularly inadequate in light of the government’s history of Section 702 violations. On four separate occasions, as recounted in [Part I of this post](#) [\[link-11\]](#), the FISA Court has found that the government was improperly handling or accessing Americans’ communications. On three of those occasions, the court held or otherwise indicated that these actions violated the Fourth Amendment. Astonishingly, *at no point in Section 702’s existence* has the government operated the program in full compliance with constitutional requirements. In light of this history, the court should have required changes far more substantial than (as the FISCR described it) “adding one (largely ministerial) item to the [FBI’s] checklist.”

After a decade of trial and error, the FISA Court should have required FBI agents to obtain warrants before searching for Americans’ communications. In my opinion, the court erred when it held that recent case law does not support a warrant

requirement for U.S. person queries of Section 702 data. Nonetheless, even if a warrant requirement were not compelled by the case law, the court still could have concluded that warrants are necessary here. In light of the repeated failure of the government, over the course of more than a decade, to adhere to the procedural requirements that the court has held the

Fourth Amendment *does* require, the court could easily have determined that nothing short of a warrant requirement will guard against the “risks of serious error and abuse” that have thus far rendered the government’s practices unconstitutional. Now that would have been a triumph of foreign intelligence surveillance oversight.

Links

link-1: two <https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/>

link-2: parts <https://www.justsecurity.org/66605/the-fisa-courts-section-702-opinions-part-ii-improper-queries-and-echoes-of-bulk-collection/>

link-3: first opinion

https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf?inline=1

link-4: second opinion

https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf?inline=1

link-5: third opinion

https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf?inline=1

link-6: It held <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf?inline=1>

link-7: it noted https://www.intelligence.gov/assets/documents/702%20Documents/oversight/20151106-702Mem_Opinion_Order_for_Public_Release.pdf?inline=1

link-8: FISA Court learned https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf?inline=1

link-9: rejected these proposals <https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf?inline=1>

link-10: reported <https://www.pclob.gov/library/702-Report.pdf?inline=1>

link-11: Part I of this post <https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/>

link-12: Image </our-work/analysis-opinion/narrowing-national-security-exception-federal-ai-guardrails-0>

link-13: Narrowing the National Security Exception to Federal AI Guardrails </our-work/analysis-opinion/narrowing-national-security-exception-federal-ai-guardrails-0>

link-14: Amos Toh </about/staff/amos-toh>

link-15: Image </our-work/analysis-opinion/how-dhss-new-social-media-vetting-policies-threaten-free-speech>

link-16: How DHS’s New Social Media Vetting Policies Threaten Free Speech </our-work/analysis-opinion/how-dhss-new-social-media-vetting-policies-threaten-free-speech>

link-17: Rachel Levinson-Waldman </about/leadership/rachel-levinson-waldman>

link-18: Melanie Geller </about/staff/melanie-geller>

link-19: How DHS Laid the Groundwork for More Intelligence Abuse [/our-work/analysis-opinion/how-dhs-laid-groundwork-more-intelligence-abuse-0](#)

link-20: A Start for AI Transparency at DHS with Room to Grow [/our-work/analysis-opinion/start-ai-transparency-dhs-room-grow](#)

link-21: More News & Analysis [/news-analysis?langcode=en](#)