

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

January 25, 2024

The Honorable Avril Haines
Director of National Intelligence
Washington, DC 20511

Dear Director Haines:

I write to request that you take action to ensure that U.S. intelligence agencies only purchase data on Americans that has been obtained in a lawful manner.

As you know, U.S. intelligence agencies are purchasing personal data about Americans that would require a court order if the government demanded it from communications companies. I first revealed in 2021 that the Defense Intelligence Agency (DIA) was purchasing, storing, and using domestic location data. Such location data is collected from Americans' smartphones by app developers, sold to data brokers, resold to defense contractors, and then resold again to the government. In addition; the National Security Agency (NSA) is buying Americans' domestic internet metadata.

Until recently, the data broker industry and the intelligence community's (IC) purchase of data from these shady companies has existed in a legal gray area, which was in large part due to the secrecy surrounding the practice. App developers and advertising companies did not meaningfully disclose to users their sale and sharing of personal data with data brokers nor seek to obtain informed consent. The data brokers that buy and resell this data are not known to consumers and several of these companies refused to answer questions from Congress regarding the companies they buy data from and the government agencies they sell it to.

The secrecy around data purchases was amplified because intelligence agencies have sought to keep the American people in the dark. It took me nearly three years to clear the public release of information revealing the NSA's purchase of domestic internet metadata. DoD first provided me with that information in March, 2021, in response to a request from my office for information identifying the DoD components buying Americans' personal data. DoD subsequently refused a request I made in May, 2021, to clear the unclassified information for public release. It was only after I placed a hold on the nominee to be the NSA director that this information was cleared for release. A copy of the NSA's letter confirming this practice is attached, as is a letter from the Under Secretary of Defense for Intelligence and Security acknowledging the purchase by

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

Defense and Intelligence Components of commercially available information, to include location data from U.S. phones.

Although the intelligence agencies' warrantless purchase of Americans' personal data is now a matter of public record, recent actions by the Federal Trade Commission (FTC), the primary federal privacy regulator, raise serious questions about the legality of this practice. On January 9, 2024, the FTC brought an action against the data broker X-Mode Social, which I first exposed in 2020 after the company's lawyers confirmed that it was selling data collected from phones in the United States to U.S. military customers, via defense contractors. The FTC held that such sensitive data sales are unlawful unless the data was obtained through consumer's informed consent.

The FTC notes in its complaint that the reason informed consent is required for location data is because it can be used to track people to "sensitive locations, including medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters." The FTC added that the "sale of such data poses an unwarranted intrusion into the most private areas of consumers' lives." While the FTC's X-Mode social complaint and order are limited to location data, internet metadata can be equally sensitive. Such records can identify Americans who are seeking help from a suicide hotline or a hotline for survivors of sexual assault or domestic abuse, a visit to a telehealth provider focusing on specific health care need, such as those prescribing and delivering abortion pills by mail, or reveal that someone likely suffers from a gambling addiction.

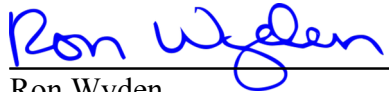
According to the FTC, it is not enough for a consumer to consent to an app or website collecting such data, the consumer must be told and agree to their data being sold to "government contractors for national security purposes." I have conducted a broad probe of the data broker industry over the past seven years, and I am unaware of any company that provides such warnings to consumers before their data is collected. As such, the lawbreaking is likely industry-wide, and not limited to this particular data broker.

The FTC's order against X-Mode Social should serve as a much-needed wake-up call for the IC. The U.S. government should not be funding and legitimizing a shady industry whose flagrant violations of Americans' privacy are not just unethical, but illegal. To that end, I request that you adopt a policy that, going forward, IC elements may only purchase data about Americans that meets the standard for legal data sales established by the FTC. I also request that you direct each IC element to take the following actions:

- Conduct an inventory of the personal data purchased by the agency about Americans, including, but not limited to, location and internet metadata. As you know, the cataloging of IC acquisition of commercially available information was also a recommendation of the Senior Advisory Group Panel on Commercially Available Information in its January 2022 report.

- Determine whether each data source identified in that inventory meets the standards for legal personal data sales outlined by the FTC. This, too, is consistent with the Senior Advisory Group’s recommendation to “identify and protect sensitive [Commercially Available Information] that implicates privacy and civil liberties concerns.”
- Where those data purchases do not meet the FTC’s standard for legal data personal data sales, promptly purge the data. Should IC elements have a specific need to retain the data, I request that such need, and a description of any retained data, be conveyed to Congress and, to the greatest extent possible, to the American public.

Sincerely,



Ron Wyden
United States Senator

CC: The Honorable Lina Khan, Chair, Federal Trade Commission



UNCLASSIFIED
NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

11 December 2023

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

(U) On December 11, 2023, Under Secretary of Defense for Intelligence and Security Moultrie wrote you to provide unclassified responses to questions you have posed to the Department of Defense (DoD) regarding the purchase and use of specific types of commercially available information (CAI). To accompany his letter, the information below provides you with additional information specific to the National Security Agency (NSA). After careful review, NSA has determined that this information is unclassified and may be released publicly.

(U) NSA understands and greatly values the congressional and public trust it has been granted to carry out its critical foreign intelligence and cybersecurity missions on behalf of the American people. To retain that trust, NSA has developed robust compliance regimes and a dedicated corporate compliance organization, and the Agency has instilled a culture of compliance within its workforce.

(U) As a Senior Advisory Group to the Office of the Director of National Intelligence recently concluded, CAI provides significant intelligence value to the U.S. Intelligence Community, including NSA. NSA's collection, acquisition, and use of CAI occurs in accordance with applicable legal and regulatory authorities to conduct lawful intelligence and cybersecurity missions. Prior to any collection, acquisition, or use of CAI, NSA ensures such activity can be done in compliance with the U.S. Constitution, as well as applicable laws, regulations, policies, procedures, and federal precedent. These include Executive Order 12333, DoD Manual 5240.01, DoD Manual S-5240.01-A, and NSA/CSS Policy 12-3 regarding the protection of civil liberties and privacy of U.S. person information when conducting NSA mission and mission-related activities. At all stages, NSA takes steps to minimize the collection of U.S. person information, to include application of technical filters. Additionally, NSA evaluates procured CAI data sets on a regular, recurring basis for uniqueness and mission value to ensure NSA continues to acquire only the most useful data relevant to mission requirements.


(U) NSA acquires various types of CAI for foreign intelligence, cybersecurity, and other authorized mission purposes, to include enhancing its signals intelligence (SIGINT) and cybersecurity missions. This may include information associated with electronic devices being used outside—and, in certain cases, inside—the United States. However, NSA does not buy and use location data collected from phones known to be used in the United States either with or without a court order. Similarly, NSA does not buy and use location data collected from automobile telematics systems from vehicles known to be located in the United States. Finally, NSA does buy and use commercially available netflow (*i.e.* non-content) data related to wholly domestic internet communications and internet communications where one side of the

UNCLASSIFIED

UNCLASSIFIED

communication is a U.S. Internet Protocol address and the other is located abroad. For example, such information is critical to protecting the U.S. Defense Industrial Base.

(U) I hope that the information provided above addresses your concerns. Please be assured that NSA will continue to implement the safeguards described in this letter, together with other applicable safeguards, to NSA's commercial data acquisitions to continue complying with all applicable laws, regulations, policies, procedures, and federal judicial precedent. Should you have any questions or require additional information, please contact NSA's Office of Legislative, State and Local Affairs.


PAUL M. NAKASONE
General, U.S. Army
Director

UNCLASSIFIED



INTELLIGENCE
AND SECURITY

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

DEC 19 2023

The Honorable Ron Wyden
U.S. Senate
Washington, DC 20510

Dear Senator Wyden:

Following up on the letters regarding the Department of Defense's potential purchase and use of specific types of commercially available information that I and Director of the National Security Agency (NSA) General Paul M. Nakasone sent you on December 11, 2023, pursuant to a request made by your staff, I am providing you with the below redacted answer to a question that I answered in my August 2, 2021, correspondence to you.

(U) Q5. Other than DIA, are any DoD components buying and using without a court order location data collected from phones located in the United States? If yes, please identify which components.

(U) (CUI) ANSWER: Among the Defense Agencies and DoD Field Activities under the authority, direction, and control of the Under Secretary of Defense (Intelligence and Security), [REDACTED] the National Security Agency, [REDACTED], buy commercial data, which includes information associated with phones located outside and inside the United States. They use the data, or a portion of the data as necessary, in accordance with applicable legal and regulatory authorities to conduct lawful intelligence or cybersecurity missions.

The above answer reflects the collective activities of multiple Defense Agencies and DoD Field Activities. Specific to the NSA alone, per GEN Nakasone's December 11, 2023, letter to you, "NSA does not buy and use location data collected from phones known to be used in the United States either with or without a court order."

Thank you for your support for the personnel of the Department of Defense. If you have questions, please contact the Office of the Assistant Secretary of Defense for Legislative Affairs.

Sincerely,


Ronald S. Moultrie



INTELLIGENCE
AND SECURITY

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

DEC 11 2023

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

I am following up on our previous correspondence regarding the Department of Defense's (DoD)'s potential purchase and use of specific types of commercially available information (CAI). Specifically, on August 2, 2021, I responded on behalf of the Secretary of Defense to your May 13, 2021, letter seeking unclassified responses to questions concerning CAI for which my office had provided classified responses. I share your commitment to ensuring that DoD adheres to U.S. law for appropriate access to, acquisition of, and use of this information in support of DoD's authorized missions. I assure you that the Department is fully committed to both the letter and the spirit of U.S. law, including the Fourth Amendment to the Constitution, and to the protection of privacy and civil liberties.

Since my August 2, 2021 response, there has been significant public interest in understanding DoD's access to, acquisition of, and use of CAI. As the Deputy Secretary of Defense has noted, with the widespread and rapid adoption of networked computing and other digital technologies, unprecedented amounts of personal information are being transmitted to commercial entities; this transmission is creating an expansive digital environment in which large volumes of sensitive data emitted from personal devices and other sources are aggregated and monetized. As with all of its activities, DoD will continue to provide Congress with a complete understanding of how DoD Components access, acquire, and use CAI in order to enable Congress to conduct oversight of our activities, regardless of the classification of those activities.

DoD Components acquire, access, and use information that is available to the American public and consumers worldwide to plan, inform, enable, execute, and support a wide range of DoD missions lawfully and responsibly, including the Department's foreign intelligence and cybersecurity missions, security activities, and to protect DoD personnel and information from foreign adversary threats. These activities are conducted in accordance with all applicable laws, including the Fourth Amendment to the Constitution, the Foreign Intelligence Surveillance Act, the Privacy Act, and DoD's implementing policies. I am not aware of any requirement in U.S. law or judicial opinion, including the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), that DoD obtain a court order in order to acquire, access, or use information, such as CAI, that is equally available for purchase to foreign adversaries, U.S. companies, and private persons as it is to the U.S. Government. DoD Components acquire and use CAI in a manner that adheres to high standards of privacy and civil liberties protections, and that accords with DoD's national security missions.

With respect to DoD personnel security, the Defense Security Components are required by law to “integrate relevant and appropriate information from various sources, including . . . publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the Director of National Intelligence.” *See* 5 U.S.C. § 11001, “Enhanced Personnel Security Programs.” In addition to this affirmative statutory obligation for DoD to collect such information, individuals also provide consent for the federal government to obtain this information about themselves when they sign the Standard Form 86, “Questionnaire for National Security.”

During the conduct of authorized intelligence activities, Defense Intelligence Components¹ follow U.S. Attorney General-approved procedures set forth in DoD Manual 5240.01, which governs the collection, retention, querying, and dissemination of United States Person Information (USPI), and rely on internal implementing policies, procedures, and guidance while carrying out their lawful intelligence missions. Defense Intelligence Components go to significant lengths to avoid ingesting or accessing USPI that could be included in CAI, and to verify that USPI is not inadvertently acquired or accessed. In these activities, Defense Intelligence Components evaluate their intelligence collection opportunities to assess whether those opportunities raise U.S. person privacy concerns, to include the collection opportunities that raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, as required by Section 3.2(e) of DoD Manual 5240.01, “Special Circumstances Collection,” and take additional steps, including obtaining authorization from the Defense Intelligence Component head or his designee before initiating such collection and applying more restrictions on the retention, querying, and dissemination. When making a determination that special circumstances exist, the Defense Intelligence Component head or his designee also must consider whether further “enhanced safeguards” are also appropriate, and if so, the Defense Intelligence Component must apply further retention restrictions in accordance with Section 3.3(g) of DoD Manual 5240.01.

Enhanced safeguards include stringent, prophylactic privacy protections that, as the term suggests, exceed the baseline handling requirements in DoD Manual 5240.01. For CAI, these enhanced safeguards are carefully tailored to mitigate the unique risks presented by the CAI at issue and can be implemented holistically across all phases of the intelligence cycle. Where enhanced safeguards are applied to mitigate the impact of DoD’s access to, acquisition of, and use of CAI on U.S. persons, DoD honors its obligation to protect the nation’s security in a manner that affirms and adheres to the fundamental values of our democracy.

In my letter to you dated August 2, 2021, I provided responses to eight questions you conveyed to DoD. I explained that responses to four of these questions—questions 4, 5, 6, and 7—were marked as Controlled Unclassified Information (CUI). Executive Order 13556

¹ “Defense Intelligence Component” is defined in DoD Manual 5240.01, but it refers to all DoD organizations that perform foreign intelligence or counterintelligence missions or functions, including the National Security Agency/Central Security Service, the Defense Intelligence Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the foreign intelligence and counterintelligence elements of the Active and Reserve Components of the Military Departments, including the United States Coast Guard when operating as a service in the Department of the Navy.

established the CUI program, which has been implemented in Part 2002 of Title 32, Code of Federal Regulations and DoD Instruction 5200.48. CUI is unclassified information that requires safeguarding and dissemination controls in accordance with law, regulation, and government-wide policy. At the time of my response, the responses to questions 4, 5, 6 and 7 contained CUI that constituted “Operations Security” information that would reveal critical information or indicators and “General Intelligence” information that would reveal unclassified intelligence activities, sources, or methods as defined in the CUI Registry maintained by the National Archives and Records Administration. After subsequent careful review, we have determined that responses to these questions as written in the August 2, 2021, letter remain properly marked as CUI. Continuing to control the August 2, 2021, responses to questions 4, 5, 6, and 7 as CUI is therefore warranted. Further, if aggregated with other unclassified or classified information acquired by foreign adversaries either publicly or through illicit means, the responses marked as CUI may give our adversaries advantageous insights. Therefore, to further the public interest, and to respond to your specific request for additional information concerning these activities that is releasable to the public, I am providing you additional releasable information regarding DoD’s access to, acquisition of, and use of CAI, including releasable answers to the questions that were answered at the CUI level in the August 2, 2021, letter.

What follows are reproduced responses to questions 1-3 and 8 as previously provided in my August 2, 2021, letter, as well as unclassified and publicly releasable answers to questions 4, 5, 6, and 7.

Q1. The Defense Intelligence Agency (DIA) recently informed Sen. Wyden’s office that they have adopted the position that the 4th Amendment, and the Supreme Court’s holding in the *Carpenter* case, do not apply to data about Americans that the government buys, and only applies to data that the government acquires via compulsion. Which other components of DoD, if any, have adopted this or a similar interpretation of the law?

ANSWER: If a DoD Intelligence Component purchases data in connection with an intelligence activity, the Component is responsible to ensure that the purchase is in accordance with existing law, regulation, and policy, including the Fourth Amendment (as understood through the *Carpenter* opinion and other relevant case law) and the Attorney General-approved procedures in DoD Manual (DoDM) 5240.01, “Procedures Governing the Conduct of DoD Intelligence Activities.

Q2. Has the DoD General Counsel’s office signed off on this legal theory and the supporting legal analysis?

ANSWER: Each DoD Intelligence Component, supported by its respective legal counsel, is responsible for ensuring that the Component’s intelligence activities are carried out in accordance with existing law (including the Fourth Amendment as understood through the *Carpenter* opinion and other relevant case law), regulation, and policy. In this case, DIA’s Office of General Counsel provided the legal support for the DIA activity.

Q3. Please provide us with a copy of the legal analysis supporting this theory. If individual DoD components have drafted their own legal analysis, please provide us a copy of each components' analysis.

ANSWER: In general, the collection and retention of data by Defense Intelligence Components enable the conduct of authorized intelligence activities (specifically, foreign intelligence and counterintelligence activities), which are subject to applicable law, regulation, and policy, including the Fourth Amendment (as understood through the *Carpenter* opinion and other relevant case law) and the Attorney General-approved procedures in DoDM 5240.01. We understand that DIA has already provided Senator Wyden's staff with a document that states DIA's legal conclusions as regards the DIA activity in question. We have no other analyses to provide in response to this question.

Q4. Please identify the DoD components that are, without a court order, buying AND using data acquired about Americans. If the DoD components do not know the identities (and citizenship) of the individuals whose information the DoD component has acquired, this question also covers the purchase and use of data about individuals / electronic devices used by individuals located in the United States.

ANSWER: DoD Components, to include Defense Intelligence Components, buy commercial data, which includes information associated with electronic devices being used outside and possibly inside the United States, to conduct lawful DoD missions, such as intelligence, personnel security, and cybersecurity. They acquire and/or access the data, or a portion of the data as necessary, in accordance with applicable legal and regulatory authorities.

Q5. Other than DIA, are any DoD components buying and using without a court order location data collected from phones located in the United States? If yes, please identify which components.

ANSWER: DoD Components, to include Defense Intelligence Components, buy CAI, which includes location data from phones located in the United States, to conduct lawful intelligence or cybersecurity missions. They acquire and/or access CAI, or a portion of the CAI as necessary, to support authorized missions or functions assigned to DoD and its components, in accordance with applicable legal and regulatory authorities.

Q6. Are any DoD components buying and using without a court order location data collected from automobile telematics systems (e.g., internet connected cars) from vehicles located in the United States? If yes, please identify which components.

ANSWER: DoD policy requires DoD components to report the acquisition of and/or access to automobile telematics systems to the Office of the Secretary of Defense. No such notification has been made.

Q7. Are any DoD components buying and using without a court order internet metadata, including "netflow" and Domain Name System (DNS) records, about:

a. domestic internet communications (where the sender and recipient are both U.S. PIIP addresses)

b. internet communications where one side of the communication is a U.S. IP address and the other side is located abroad.


ANSWER: DoD Components, to include Defense Intelligence Components, acquire, access, and use commercially available netflow data concerning the communications described in subparts (a) and (b) above in order to enhance their intelligence and/or cybersecurity missions, and in doing so, may purchase CAI that contains metadata reflecting communications in which one or both Internet Protocol addresses are located within the United States.

Q8. If the answers to 5, 6, or 7 are yes, have these activities been reviewed by the DoD inspector general? If not, has DoD notified the inspector general that they are taking place?

ANSWER: All entities provided an answer that these activities have not been reviewed, as it is not Department policy to request a review by the Office of the Inspector General of all DoD activities.

Thank you for your support for the personnel of the Department of Defense.

Sincerely,


Ronald S. Moultrie