S. HRG. 119–259

THREATS AND CHALLENGES POSED TO DOD PERSONNEL AND OPERATIONS FROM ADVERSARIAL ACCESS TO PUBLICLY AVAILABLE DATA COUPLED WITH ADVANCED DATA ANALYSIS TOOLS NOW WIDELY AVAILABLE ON THE COMMERCIAL MARKET

HEARING

BEFORE THE

SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

OCTOBER 7, 2025

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
62–460 PDF WASHINGTON : 2026

COMMITTEE ON ARMED SERVICES

ROGER F. WICKER, Mississippi, *Chairman*

DEB FISCHER, Nebraska	JACK REED, Rhode Island
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI K. ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
KEVIN CRAMER, North Dakota	TIM KAINE, Virginia
RICK SCOTT, Florida	ANGUS S. KING, Jr., Maine
TOMMY TUBERVILLE, Alabama	ELIZABETH WARREN, Massachusetts
MARKWAYNE MULLIN, Oklahoma	GARY C. PETERS, Michigan
TED BUDD, North Carolina	TAMMY DUCKWORTH, Illinois
ERIC SCHMITT, Missouri	JACKY ROSEN, Nevada
JIM BANKS, Indiana	MARK KELLY, Arizona
TIM SHEEHY, Montana	ELISSA SLOTKIN, Michigan

JOHN P. KEAST, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

JONI K. ERNST, Iowa, *Chairman*

TOM COTTON, Arkansas	ELISSA SLOTKIN, Michigan
MIKE ROUNDS, South Dakota	JEANNE SHAHEEN, New Hampshire
KEVIN CRAMER, North Dakota	KIRSTEN E. GILLIBRAND, New York
MARKWAYNE MULLIN, Oklahoma	TIM KAINE, Virginia
TED BUDD, North Carolina	GARY C. PETERS, Michigan
ERIC SCHMITT, Missouri	JACKY ROSEN, Nevada
TIM SHEEHY, Montana	MARK KELLY, Arizona

CONTENTS

OCTOBER 7, 2025

THREATS AND CHALLENGES POSED TO DOD PERSONNEL AND OPERATIONS FROM ADVERSARIAL ACCESS TO PUBLICLY AVAILABLE DATA COUPLED WITH ADVANCED DATA ANALYSIS TOOLS NOW WIDELY AVAILABLE ON THE COMMERCIAL MARKET

TUESDAY, OCTOBER 7, 2025

UNITED STATES SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:28 p.m., in room SR–222, Dirksen Senate Office Building, Senator Joni Ernst (Chairwoman of the Subcommittee) presiding.

Subcommittee Members present: Senators Ernst, Slotkin, Kaine, and Peters.

OPENING STATEMENT OF SENATOR JONI ERNST

Chairwoman ERNST. We will go ahead and get started this afternoon, and we may be joined by other Members. I know we have a pretty full schedule this afternoon, so thank you.

Good afternoon. The Subcommittee on Emerging Threats and Capabilities meets today to receive testimony on how our adversaries are using publicly available data to undermine the security of Department of Defense (DOD) personnel, platforms, and operations. As our lives become increasingly connected, the invisible trail of metadata, location signals, app usage, biometric data, and other digital breadcrumbs has created a new exploitable surface for adversaries. Data that seems insignificant on its own can, when aggregated with other information and intelligence, reveal troop movements, operational planning, and the daily routines of our personnel.

Foreign intelligence services and cybercriminals can harvest and analyze this information in ways that threaten the security of DOD missions and the safety of our servicemembers and their families. We have seen in public news reports how the use of commercially available fitness apps has inadvertently exposed the location of sensitive military bases. We have seen how social media and mobile devices have been used to geolocate personnel and manipulate their information environment.

The pace of technology and the widespread use of Internet-connected devices presents a significant and evolving challenge. Today, we will hear from experts across the government and industry to understand the scope of this threat and what must be done. Thank you.

With that, then I will turn to the Ranking Member.

STATEMENT OF SENATOR ELISSA SLOTKIN

Senator SLOTKIN. Great. Thank you, Senator Ernst, for holding this really important hearing. Thank you to our guests for joining us and helping us parse through this.

I think, you know, for those of us who watch the national security space really closely, I think it is very clear that the future of warfare may not be tanks and airframes, but really data and who controls that data, who can easily amalgamate that data and then weaponize that data. While there are lots of actors out there, we certainly know that China is just a massive player in this space and, in my opinion, has already, both through commercially available information but also through the theft of personal information, really made a business of collecting this data for a whole bunch of reasons. I think something like in the order of $600 billion annually is lost in intellectual property that is taken from U.S. companies through cyber attacks, so it is a real threat, even if it is hard to get our hands around.

There is, I think, lots of good bipartisan work going on on this in the National Defense Authorization Act (NDAA) and other spaces, but I think this is a great opportunity to highlight for the American public kind of the nature of changing warfare and how their own personal data is now on the frontlines in a very, very different way, so look forward to hearing the conversation.

Back over to you, Madam Chairwoman.

Chairwoman ERNST. Wonderful. Thank you. I will just start with some brief introductions of our witnesses today, and then you will each be recognized for your statements. You will each have 5 minutes for opening statements.

We have Dr. Joseph Kirschbaum, and he is the director in the Defense Capabilities and Management team at the U.S. Government Accountability Office (GAO), where he oversees evaluations of defense and intelligence programs for congressional committees. So thank you very much for being here today, Dr. Kirschbaum.

Justin Sherman is the founder and Chief Executive Officer (CEO) of Global Cyber Strategies, a Washington, DC-based research and advisory firm specializing in cybersecurity, data privacy, technology policy, and geopolitics for clients ranging from startups to the U.S. Government. Thank you very much for being here, Mr. Sherman.

John Doyle is the founder and CEO of Cape, a privacy-first mobile carrier designed to defend users' mobile identity and limit the data exposure inherent in traditional cellular networks. So thank you very much for being here, Mr. Doyle.

Then finally, Michael Stokes is vice president of strategic engagements and marketing at Ridgeline International, where he leads business development, partner growth, and market strategy efforts

in the cybersecurity and digital signature management space. Thank you very much, Mr. Stokes.

With that, we will start with you, Dr. Kirschbaum, and you are recognized for 5 minutes.

STATEMENT OF JOSEPH W. KIRSCHBAUM, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Dr. KIRSCHBAUM. Chairwoman Ernst, Ranking Member Slotkin, and Members of the Subcommittee, I am pleased to be here today to discuss the report which we will be issuing today on risks of publicly available information to the Department of Defense's personnel and operations and their approach to address those risks. We have previously reported how the escalation in the volume and interconnectedness of data and the evolving DOD information environment have changed the national security landscape. Historically, enemies who seek harm to U.S. Forces or its people had to go where the information was and find ways to get at it, you know, rifling through the trash, sustained surveillance, and other techniques. These days, in the information age, all that data and much more comes to them, which lowers the bar of entry for malicious actors.

At the heart of the matter is the fact that DOD servicemembers, employees, contractors, family members constantly provide massive amounts of traceable data, known as the digital footprint, and do so intentionally and unintentionally. This data can be collected and aggravated by the public, data brokers, or malicious actors over time that create a digital profile that can reveal potentially sensitive and classified information.

We are talking here about a mix of data and information. This includes social media posts, official media releases, public information, property records, transmissions from personal electronic devices, electronic emissions from military platforms themselves, and other examples. The availability of these data and potential for them to be exploited are increased by data brokers with both neutral and nefarious intent and the application of artificial intelligence (AI).

For our report, we develop notional threat scenarios that exemplify how malicious actors can collect and use information about DOD operations and its personnel. We develop these based on analyses of literature, interviews, and information from the Department of Defense, and by conducting our own investigation into the types and sources of these data.

Two of the scenarios are shown to my right and your left, and there are in the handouts in front of you. The first is a depiction of publicly available information presenting a force protection threat to a servicemember and/or family members through the aggregation of information and sources. A servicemember's name, rank, photograph, and unit can be identified from online sources. DOD websites and social media often post this information freely.

From there, a malicious actor can narrow their search by visiting servicemembers or relative social media sites and associated information and data tags. From there, you can start collecting additional information, especially if one of the individuals has a phone

that allows identification by nearby devices or if they have downloaded a third-party application that tracks geolocation, as many of them do. Like puzzles, these can be set into place to show pattern of life.

In testing this scenario, our investigators didn't have to proceed far into the internet or the dark web to find access to data brokers selling significant quantities of additional information on military personnel.

The next is a depiction of risks to naval operations through exposure of real-time information about a ship's movements, its personnel, and onboard conditions. Taken collectively, information from Navy and DOD posts and press releases and seemingly private blogs and posts can be linked with open transmissions from ship and aircraft platforms, as well as personal connected devices to project the route of an aircraft carrier and present a nefarious actor with a useful intelligence picture.

Our report also illustrates two other scenarios, risk to military capabilities from training operations and equipment, information and risks to military leadership from potential disclosure of an official's behaviors and associations. As with previous information environment challenges, DOD has no single officer entity to address all risks associated with the kind of thing we are talking about here, nor should it. DOD has security disciplines and functions to manage these kinds of risks. We found uneven progress among these areas to address the risks we identified. This is about policy, organization, and culture. Our forthcoming report issued today recommends that DOD improve policies, guidance, training, and assessments across those security disciplines, and DOD has already agreed with those recommendations.

In conclusion, DOD has an opportunity to make progress. This will require them to look beyond what is strictly in their control in terms of official data and information and what might not be. That in turn will help the Department determine how best to mitigate those threats.

This completes my prepared statement, and I am happy to address any questions.

[The prepared statement of Mr. Kirschbaum follows:]

United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. ET
Tuesday, October 7, 2025

INFORMATION ENVIRONMENT

DOD Faces Risks with Publicly Accessible Information

Statement of Joseph W. Kirschbaum, PhD
Director, Defense Capabilities and Management

GAO-26-108771

Chairwoman Ernst, Ranking Member Slotkin, and Members of the Subcommittee:

I am pleased to be here today to discuss the risks of the growing use of electronic devices and online activities by the Department of Defense's (DOD) personnel and their operations. Throughout the day, people—including DOD service members, employees, contractors, and family members— leave behind massive amounts of traceable data that can be collected and aggregated by the public, data brokers, and malicious actors. These data, in the aggregate, can undermine national security and pose significant security, privacy, and safety risks.

All of this digital activity generates volumes of traceable information—also known as a *digital footprint*. Over time, multiple footprints can create a *digital profile* that can reveal potentially sensitive or classified information. We have previously issued reports highlighting how this escalation in volume, the interconnectedness of data, and the evolving DOD information environment have changed the landscape of information and national security.[1]

My testimony summarizes our pending report entitled *Information Environment: DOD Needs to Address Security Risks of Publicly Accessible Information*.[2] This statement focuses on (1) risks of publicly available data about DOD personnel and operations, and (2) DOD's approach to address security-related risks.

In conducting our work, we developed and examined threat scenarios that depict potential consequences from the exploitation of publicly accessible digital data. We developed these scenarios based on analyses of literature research, interviews, and our own investigation. We also collected and reviewed information from officials from the Office of the Secretary of Defense and a non-generalizable sample of 10 DOD components. Our work was performed in accordance with generally accepted government auditing standards. We conducted our related investigative work in accordance with investigation standards prescribed

[1]GAO, *Information Environment: Opportunities and Threats to DOD's National Security Mission*, GAO-22-104714 (Washington, D.C.: Sep. 21, 2022); *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft*, GAO-18-177 (Washington, D.C.: Jan. 18, 2018); and *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-514SU (Washington, D.C.: June 7, 2017).

[2]GAO will publish this report once the agency resumes operations.

by the Council of the Inspectors General on Integrity and Efficiency. More detailed information on the scope and methodology of our work can be found in our report.

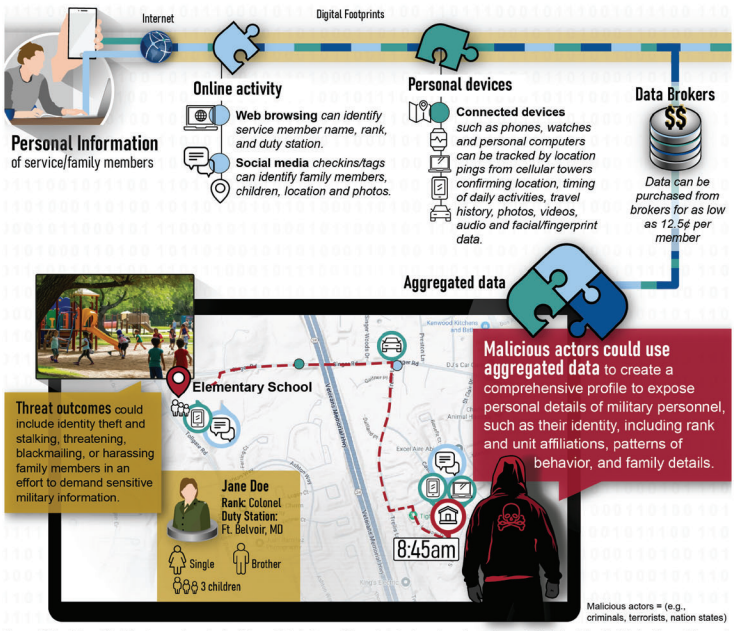
Malicious Actors' Access to Digital Information of DOD Personnel and Operations Poses Growing Risk

DOD officials and documents identify the public accessibility of digital data as a real and growing threat that poses risks to personnel privacy and safety, mission success, and national security. To illuminate this threat, we developed notional threat scenarios that exemplify how malicious actors can collect and use digital information about DOD operations and its personnel that appears in the public domain.

- **Risk to personnel and their families:** Exposure of personal information such as identity, rank, unit affiliation, patterns of behavior, and family details.
- **Risk to naval operations:** Disclosure of real-time intelligence about a ship's movements, personnel, and onboard conditions.
- **Risk to military capabilities:** Identification of vulnerabilities in military training, operations, and equipment.
- **Risk to leadership:** Disclosure of a military official's behaviors and associations to predict their movements and objectives.

For example, figure 1 shows how digital information purchased from data brokers or collected from the web could be used to identify and harm DOD personnel and their families.

Figure 1: Scenario of Threat Outcomes from Exposure of DOD Personnel Information

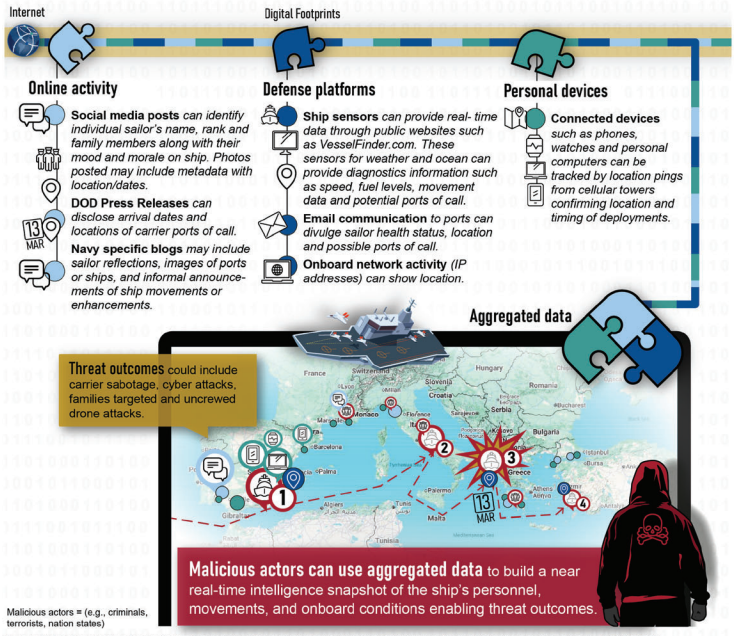


Sources: GAO analysis and illustrations (person at computer, hand/phone, data broker icon, malicious actor, internet, puzzle, monitor, service member illustrations), SaroStock/stock.adobe.com (playground photo), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-108771

9

Figure 2 provides an illustration of how digital information could be used by malicious actors to potentially project the route of an aircraft carrier and disrupt naval operations. This information can be collected from sources including social media posts, DOD press releases, and blogs.

Figure 2: Scenario of Threat Outcomes from Disclosure of Naval Operations



Sources: GAO analysis and illustrations (malicious actor, internet, puzzle, monitor illustrations), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-108771

In our review of risk to military capabilities, we note that cybersecurity researchers found forum discussions on the dark web that included advertisements for military manuals on tank operations and improvised explosive device training. Also, our investigators found a social media post with videos of military jump training, including live military flights, internal views of the aircraft, and equipment used by the paratroopers. The training manuals could be purchased from the dark web.

In our review of risk to leadership, we identified a scenario in which an Army official traveling to a high-profile military conference downloaded a video game for their child to use during their travel. However, the application had extensive access to sensitive information and functions on the official's phone, including location, credit card, contacts, camera and microphone, SMS messages, and network access.

DOD Has an Established Approach to Manage Security-Related Risks but Needs to Take Additional Actions

DOD's Approach to Managing Security-Related Risks

DOD has established security disciplines and related functions to manage risks. These disciplines and functions include (but are not limited to) counterintelligence, antiterrorism (force protection), insider threat, mission assurance, operations security, and critical program information protection. The advantages of having security disciplines are the department could use existing structures, doctrine, and policy to build in new considerations. Conversely, the expansive and separate nature of this structure can result in uneven progress.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

Force protection: Preventive measures taken to mitigate hostile actions against Department of Defense (DOD) personnel (including family members), resources, facilities, and critical information.

Insider threat: A threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of DOD and knowingly or unknowingly commits an act in contravention of law or policy that resulted in or might result in harm through the loss or degradation of government or company information, resources, or capabilities, or a destructive act, which may include physical harm to oneself or another.

Mission assurance: A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains critical to the execution of DOD mission-essential functions in any operating environment or condition.

Operations security: An activity that identifies and controls critical information and indicators of friendly force actions.

Critical program information protection: U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

Source: GAO analysis of DOD documents. | GAO-26-108771

To manage security-related risks, DOD has assigned senior-level officials within the Office of the Secretary of Defense who provide policies, procedures, and guidance on how to limit the amount and type of digital information that is accessible to the public. Specifically, the

- Under Secretary of Defense for Intelligence and Security establishes and oversees the implementation of policies and procedures for security areas such as DOD counterintelligence, insider threat, operations security, and program protection.[3]
- Under Secretary of Defense for Policy establishes and oversees the implementation of policies and procedures for DOD mission assurance and antiterrorism, which includes force protection.[4]
- Under Secretary of Defense for Research and Engineering establishes policies for development and approval of systems engineering plans and program protection plans, among other things.[5]

[3]DOD Directive 5143.01, *Under Secretary of Defense for Intelligence and Security (USD(I&S))* (Oct. 24, 2014) (incorporating change 2, Apr. 6, 2020).

[4]DOD Directive 5111.01, *Under Secretary of Defense for Policy (USD(P))* (June 23, 2020) and DOD Instruction 2000.12, *DOD Antiterrorism Support to Force Protection* (June 11, 2025).

[5]DOD Directive 5137.02, *Under Secretary of Defense for Research and Engineering (USD (R&E))* (July 15, 2020).

- Assistant Secretary of Defense for Public Affairs acts as the sole authority for releasing DOD information and visual information materials, including press releases.[6]
- DOD Chief Information Officer develops the department's cybersecurity policy and guidance.[7]

In addition, DOD components are responsible for implementing DOD issuances to protect information, personnel, equipment, and operations.[8] Some examples:

- Military departments conduct training and assessments on operations security.
- Defense Counterintelligence and Security Agency provides security training.

Moreover, DOD has established other organizations, such as the Defense Security Enterprise Executive Committee.[9] The committee includes stakeholders from across the department, as shown in figure 3.

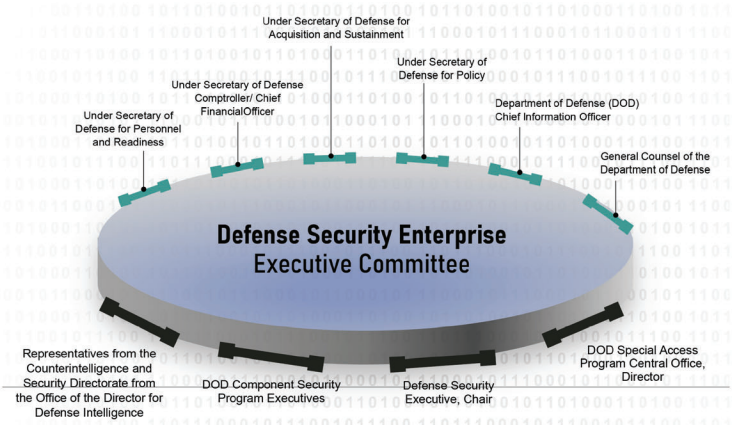
[6]DOD Directive 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))* (Aug. 7, 2017).

[7]DOD Directive 5144.02, *DOD Chief Information Officer (DOD CIO)* (Nov. 21, 2014) (incorporating change 1, effective Sept. 19, 2017).

[8]DOD defines "DOD components" as the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the DOD Office of Inspector General, the defense agencies, the DOD field activities, and all other organizational entities within DOD.

[9]DOD Directive 5200.43, *Management of the Defense Security Enterprise* (Oct. 1, 2012) (incorporating change 3, effective July 14, 2020).

Figure 3: Defense Security Enterprise with Senior-Level DOD Officials Across Security Disciplines and Functions



Source: GAO analysis of DOD documents. | GAO-26-108771

DOD Needs to Take Action to Reduce Risks of Publicly Accessible Digital Data

DOD has taken some actions that address risks associated with publicly available information about DOD operations and personnel. For example,

- The DOD Chief Information Officer issued a policy prohibiting military personnel, civilian employees, and contractor personnel from using personal email or other nonofficial accounts to exchange official information. [10]

[10]DOD Instruction 8170.01, *Online Information Management and Electronic Messaging* (Jan. 2, 2019) (change 2, Mar. 12, 2025).

- The Assistant to the Secretary of Defense for Public Affairs issued a policy providing core principles and guidance on social media use, along with guidance for social media records management.[11]
- The Defense Information Systems Agency has incorporated digital profile risks in the DOD-wide cybersecurity training that every employee is supposed to complete annually.
- A Joint Staff organization, known as Joint Staff Operational Security Element, hosted a week-long conference in 2025 that highlighted the OPSEC risks associated with digital profile.

Several DOD components administer training that touches upon risks associated with digital profiles. For example, the Defense Intelligence Agency's Joint Counterintelligence Training Academy offers a course on understanding remote surveillance (also known as ubiquitous technical surveillance) and how the five pathways of collection (see text box) integrate to pose a threat to intelligence activities.

Ubiquitous technical surveillance is the collection and long-term storage of data in order to analyze and connect individuals with other people, activities, and organizations. Ubiquitous technical surveillance is organized into five pathways of collection:

- Online (e.g., internet searches and websites)
- Electronic (e.g., Bluetooth connections, GPS information, and smart devices)
- Financial (e.g., banking applications and tap to pay)
- Visual-physical (e.g., CCTV cameras and smart doorbell)
- Travel (e.g., flight itineraries and GPS location searches)

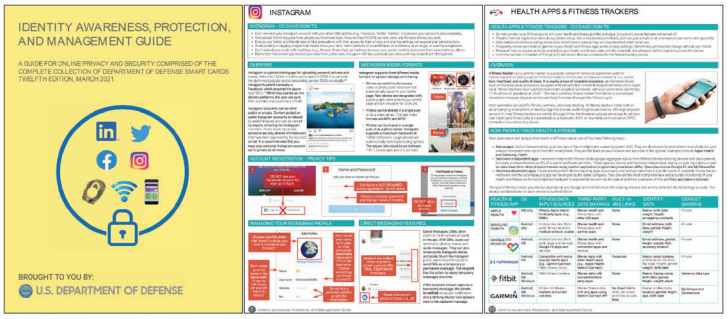
Source: International Journal of Trend in Scientific Research and Development. | GAO-26-108771

- DOD components have developed posters, smartcards, or other awareness documents to help employees understand how to keep their identities private and secure online.[12] This collection of smartcards provide an individual the tools, recommendations, and step-by-step guides for implementing settings that maximize their security in a variety of digital sources, such as Facebook, fitness trackers, online dating services, and smartphones (see figure 4).

[11]DOD Instruction 5400.17, *Official Use of Social Media for Public Affairs Purposes* (Aug 12, 2022) (incorporating change 2, Feb. 14, 2025).

[12]*Identity Awareness, Protection, and Management Guide*, Washington, D.C., accessed September 22, 2025, https://www.odni.gov/files/NCSC/documents/campaign/DoD_IAPM_Guide_March_2021.pdf.

Figure 4: Example of Department of Defense's Smartcards on Securing Digital Profiles



Source: DOD Identity Awareness, Protection, and Management Guide. | GAO-26-108771

However, most of DOD's efforts to address the risks have almost exclusively been through DOD's OPSEC program and not the other security disciplines. The scenarios discussed above highlight that public accessibility of digital information impacts multiple security disciplines—including OPSEC, counterintelligence, force protection, mission assurance, program protection. For example:

- The offices of the Under Secretary of Defense for Policy (responsible for force protection and mission assurance) and the Under Secretary of Defense for Research and Engineering (responsible for program protection) do not have any policies or guidance that identify actions DOD personnel and contractors should take to reduce risks associated with the public accessibility of digital information.
- Most (80 percent) of the training that DOD officials identified as educating DOD personnel about the digital profile, its associated risks, and best practices for countering risks, primarily focused on OPSEC. Training and awareness programs, according to the former Director of National Intelligence, are the most important weapons in the cyber-battlefield when it comes to personal devices and accounts.

In addition, OSD offices had limited collaboration to address risks associated with the digital profile—such as through the Defense Security Enterprise Executive Committee. The executive committee is a cross-functional governance body that includes stakeholders from across the department, including the General Counsel. So, the executive committee is well-positioned to support and facilitate efforts to reduce risk. Furthermore, multiple DOD components that we included in the scope of our review had not completed required security assessments, nor assessed the risks associated with the public accessibility of digital information.

In the forthcoming report, we made 12 recommendations to DOD to address these issues. Among our recommendations is that DOD:

- assess existing departmental security policies and guidance and make recommendations to the Secretary of Defense on updating policy and guidance;
- improve collaboration across the department to reduce the risks of information about DOD and its personnel becoming publicly accessible;
- review and assess security training to ensure that digital profile issues are considered in all security areas, and make appropriate recommendations; and
- ensure components are conducting required security assessments.

DOD concurred with 11 of the 12 recommendations and partially concurred with one recommendation. DOD also identified initial actions to implement them.

In conclusion, DOD has an opportunity to address risks affecting its personnel and operations by taking additional actions. By implementing our recommendations, DOD can improve the representation of digital profile threats in its existing policies and guidance. Also, DOD can ensure that digital profile issues are considered in training for all security areas: counterintelligence, force protection, insider threat, mission assurance, operational security, and program protection. Lastly, by conducting required security assessments DOD components can decrease the risk of not detecting vulnerabilities that malicious actors could otherwise exploit.

Chairwoman Ernst, Ranking Member Slotkin, and members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Joseph W. Kirschbaum, Director, Defense Capabilities and Management, at Kirschbaumj@gao.gov; or Marisol Cruz Cain, Director, Information Technology and Cybersecurity, CruzCainm@gao.gov.

Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Tommy Baril and Lee McCracken (Assistant Directors), Ashley Houston (Analyst-in-Charge), Nicole Ashby, Prianka Bose, Chris Businsky, Ash Huda, Claire Liu, Richard Powelson, and Angel Zollicoffer. Tracy Barnes, Mark MacPherson, Mike Silver, and Pamela Snedden also provided support to this testimony.

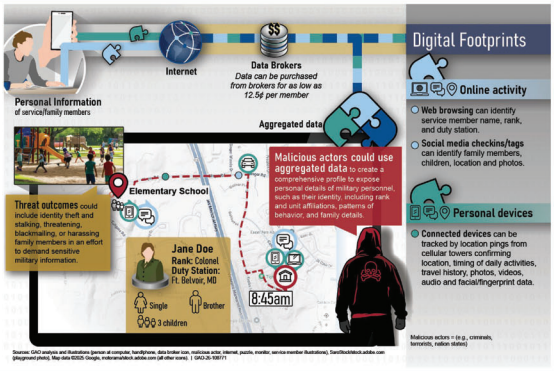
GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on X, LinkedIn, Instagram, and YouTube. Subscribe to our Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454
Media Relations	Sarah Kaczmarek, Managing Director, Media@gao.gov
Congressional Relations	A. Nicole Clowers, Managing Director, CongRel@gao.gov
General Inquiries	https://www.gao.gov/about/contact-us

[Supporting documentation supplied by GAO to follow:]

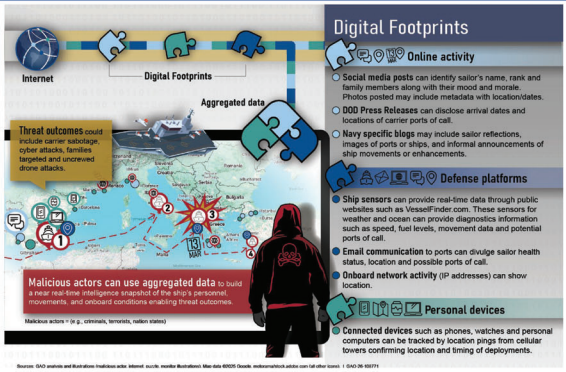
GAO

Graphics Focused on DOD Risks Associated with Publicly Accessible Information

GAO Figure 1: Scenario of Threat Outcomes from Exposure of DOD Personnel Information



GAO Figure 2: Scenario of Threat Outcomes from Disclosure of Naval Operations



GAO Figure 3: Notional Digital Profile Threat Scenario Exposing DOD-Related Training Materials and Military Capabilities

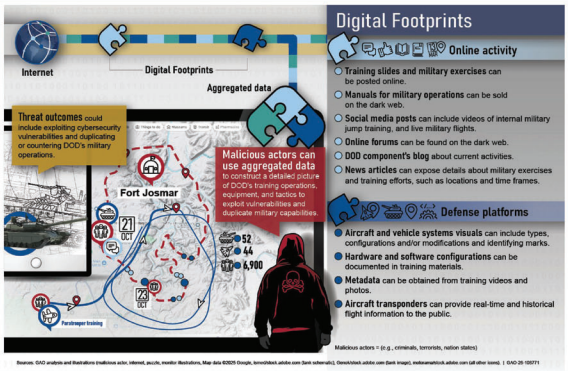
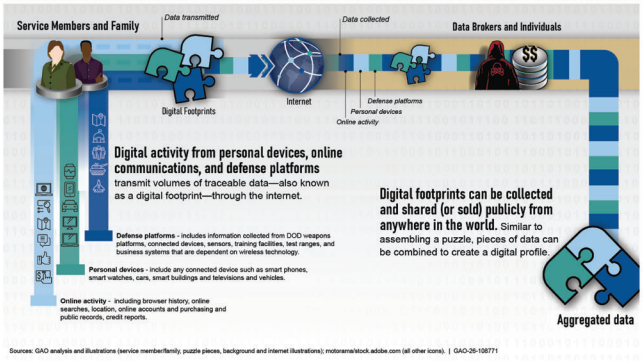
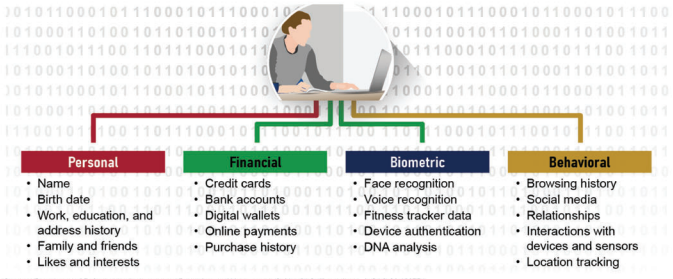


Figure 4: Digital Activity Generates Digital Footprints That Are Transmitted Through the Internet

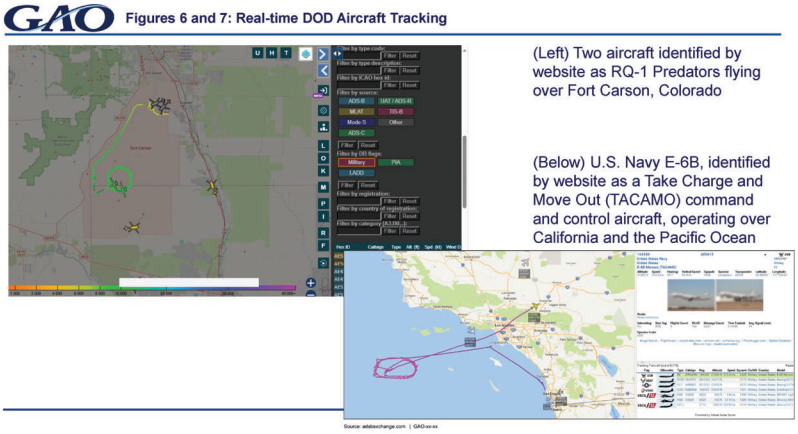


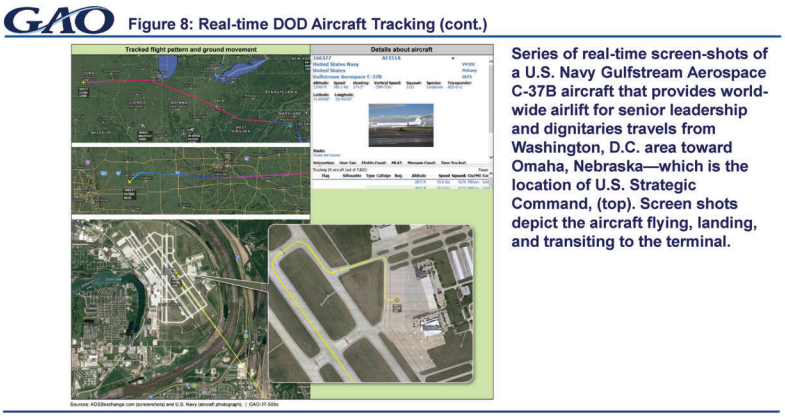
Sources: GAO analysis and illustrations (service member/family, puzzle pieces, background and internet illustrations); motorama/stock.adobe.com (all other icons). | GAO-26-108771

Figure 5: People (Un)Wittingly Leave Behind Sensitive Information



Sources: Department of Defense Identity Awareness, Protection, and Management Guide, GAO (illustrations). | GAO-26-108771





Chairwoman ERNST. Thank you, Dr. Kirschbaum.

Mr. Sherman, you are now recognized for 5 minutes.

STATEMENT OF JUSTIN SHERMAN, FOUNDER AND CHIEF EXECUTIVE OFFICER, GLOBAL CYBER STRATEGIES

Mr. SHERMAN. Subcommittee Chairwoman Ernst, Ranking Member Slotkin, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today about the explosion in data, digital connectivity, adversary threats, and how the U.S. can respond.

In my work, I have published at length on the risks of the data ecosystem to national security, have worked on several U.S. Government responses to the problem, and also teach at Georgetown, graduate students on open source intelligence, commercial data, and U.S. national security strategy.

In the last 2 decades, the amount of data and digital connectivity has exploded, both in the U.S. and globally. This has afforded the

U.S. a number of advantages in intelligence, military, and security areas, but we are unfortunately significantly behind when it comes to recognizing the threats these pose to the United States and to the servicemembers and other U.S. national security personnel that make a tremendous sacrifice in their public service, including, for many, putting their lives on the line every single day.

In our current digital environment, a tremendous amount of data is collected, analyzed, and transmitted near incessantly on virtually every single American—health information, device IDs, 24/7 phone location data, records of online purchases, browsing histories, pornography consumption, propensities for cigarettes or alcohol, late-night gambling, or overseas travel. There are several dimensions to this risk: Open-source information on public websites, social media pages, the dark web, and even freely available commercial satellite imagery platforms; data brokers that collect and sell thousands of data points per person on hundreds of millions of Americans; real-time bidding networks for online ads that constantly blast out device-identifiable sensitive data every single day; vehicles that transmit location signals every few seconds, accurate within inches; and even commercial data analysis capabilities that allow adversaries the ability to identify, reidentify, and package up Americans' data.

All of this can be exploited in cyber, information, intelligence, and other operations against the United States and represents an extraordinary counterintelligence threat. We have already seen examples of how this threat has impacted U.S. national security. The U.S. Government calls this the UTS or ubiquitous technical surveillance problem.

A few examples. The 2018 Strava scandal, as the chair mentioned, showed how one web application could expose the real-time locations and historical locations of United States troops, including those jogging around forward-operating bases in Afghanistan. I ran a Defense Department-funded threat assessment where my research team set up websites in the United States and Singapore, contacted U.S. data brokers, and bought individually identified, highly sensitive health, financial, and other data on thousands of Active Duty U.S. military servicemembers with virtually no serious background checks or vetting for as low as 12 cents a servicemember and even were able to geofence the data to bases publicly known to house U.S. Special Operations Forces. They also transferred this data overseas.

A 2023 study identified real data packages in advertising systems right now with titles such as "people who work in the Pentagon," "people working in defense and space," and individuals labeled as government, intelligence, and counterterrorism.

Foreign adversaries such as China and Russia are readily investing to be able to exploit these vulnerabilities. Beijing has stolen enormous volumes of data on Americans, has advanced cyber and AI capabilities, and has shown a strong OSINT interest in United States Military Forces. Moscow, likewise, has advanced cyber and intelligence functions and many open source intelligence (OSINT) and cyber contractors it can throw at this work.

Given the threats, there are three steps that Congress can take now. First is to compel the Defense Department to evaluate these

risk mitigation gaps, both in open-source/unclassified as well as classified reports and both enterprise-wide as well as within and between specific agencies.

The second is to pass legislation to further lock down Americans' data, building on recent efforts at the Department of Justice and in last year's Congress with the bipartisan Protecting Americans' Data from Foreign Adversaries Act or PADFAA, among other things.

Third is to help rethink the U.S. societal attitude. For decades, we have seen the consequences of this connect now, think later, download now, assess the risk later attitude, both in society generally and with respect to our military. Rethinking this is essential to national security and to the future.

So acting now is not just essential for our military servicemembers whose lives are on the line, but also to the Defense Department's vital mission set and broader U.S. national security interests. Thank you.

[The prepared statement of Mr. Sherman follows:]

Protecting U.S. National Security and U.S. Personnel from Ubiquitous Technical Surveillance and Commercial Data Exploitation

Written Testimony

Justin Sherman
Founder and CEO, Global Cyber Strategies

U.S. Senate Committee on Armed Services

Subcommittee on Emerging Threats and Capabilities

Hearing on "Threats and Challenges Posed to Department of Defense Personnel and Operations from Adversarial Access to Publicly Available Data Coupled with Advanced Data Analysis Tools Now Widely Available on the Commercial Market"

October 7, 2025

Subcommittee Chair Ernst, Ranking Member Slotkin, and distinguished members of the Subcommittee, I appreciate the opportunity to testify today about the explosion in data and digital connectivity, adversary threats and risks to U.S. national security, and how the U.S. can respond.

I am the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm. I also teach at Georgetown and am a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative, among other hats. I consult, teach, research, and write on cybersecurity and data privacy, technology policy, and geopolitics, with substantial work focused on open-source intelligence (OSINT), commercial data, and various opportunities for and especially risks to the United States—including advising the U.S. government on the issues at play.

In the last two decades, the volume of open-source information in the world, the amount of commercial data available on the United States, and the degree of digital connectivity in the United States and around the world have exploded. This has afforded the U.S. government a number of opportunities and potential advantages in military and intelligence operations. Simultaneously, our country has unfortunately been woefully behind in recognizing the threats all this information, data, and connectivity pose to our national security—including our servicemembers and other Americans serving our country in the national security community. Foreign adversaries such as China and Russia, meanwhile, are investing readily to be able to exploit these vulnerabilities.

Congress should compel the Defense Department to evaluate risk mitigation gaps, pass legislation to lock down Americans' data, and help rethink the U.S.' "connect now, assess latter" attitude.

In this written testimony, I describe how:

- In the last two decades, the amount of data collected, analyzed, and transmitted every day exploded—alongside an explosion in digital connectivity in the United States and around the world. This data and digital connectivity has included open-source information, commercial data, real-time bidding networks, smartphones, wearable devices, vehicles, internet and digital networks, and commercial data analytic capabilities.
- This has afforded the U.S. government a number of opportunities and potential advantages in military and intelligence operations. Simultaneously, the United States is unfortunately behind in recognizing the threats all this information, data, and connectivity pose to national security—including U.S. military servicemembers and all other Americans who serve their country, from diplomats to intelligence personnel to scientists to contractors.
- Foreign adversaries can leverage all this data and digital connectivity against the Defense Department, the U.S. national security community, and U.S. national security broadly—spanning cyber operations, counterintelligence threats, malign information targeting, data analysis and reidentification, anomalous behavior identification, and, among others, profiling individuals, sites, activities, and capabilities.
- In 2018, for example, a wearable device-linked software application was found to be exposing many users' location histories—their logged movements around the world—on a publicly viewable website. Researchers used the data to track what appeared to be U.S. military servicemembers moving around forward operating bases in Afghanistan.
- In 2023, for example, an analysis of real-time bidding segments found advertising packages available for use with titles such as "People who work in the Pentagon," "Department of Defense," "People working in defense & space," and "People who work in the military" as well as individuals categorized as "Government – Intelligence and Counterterrorism."
- The U.S. government has come to use the phrase "ubiquitous technical surveillance" to describe this digital and data threat environment. Some within the CIA, according to a Justice Department report, have described the threat as "existential." Reports from the Government Accountability Office, MITRE, and others indicate the many challenges at play, ranging from social media data to data brokers to digital advertising networks.
- Foreign adversaries, such as China and Russia, are investing readily to be able to exploit these vulnerabilities across the explosion of data and digital connectivity—and to leverage commercial data analytic capabilities and more to their own advantages.
- Beijing has embarked on an "ambitious national data strategy," has sophisticated cyber and technology capabilities, has stolen enormous volumes of data on Americans in recent years that could be analyzed with AI and other technologies, and has built out an extensive domestic surveillance apparatus, among others. One report illustrates the Chinese military's interest in collecting OSINT on a range of specific topics related to the U.S. military, its personnel, its capabilities, its concepts, and its operations.
- Moscow has sophisticated cyber and intelligence capabilities, OSINT-practicing companies, investments in AI, and an expanding domestic surveillance system with AI facial recognition on CCTV networks and a growing biometric surveillance infrastructure.
- Given the threats, there are growing discussions about potential ways for the U.S. government to better mitigate UTS and better protect the data—and, ultimately, safety and security—of U.S. national security personnel, the government, and the country itself.

A Data and Digital Explosion

In the last two decades, the amount of data collected, analyzed, and transmitted every day exploded—alongside an explosion in digital connectivity in the United States and around the world. This data and digital connectivity has included, among other elements:

- *Open-source information* available on, or via, websites, social media platforms, traditional media with an online presence, property filings, business records, dark web sources, freely available commercial satellite imagery platforms, and much more;[1]
- *Commercial data* gathered and sold by data brokers, or companies in the business of collecting, inferring, analyzing, packaging, and selling data, including individually identified or easily identifiable data concerning individuals' demographic characteristics, political preferences and beliefs, finances, health conditions, browsing activity, shopping habits, travel activities, social media accounts, connected devices and digital identifiers, 24/7 phone geolocation signals, employment information, vehicle data, and much more;[2]
- *Real-time bidding (RTB) networks* for online ads that intake a wide range of data points on digital device users to whom an advertiser might want to run a targeted ad—such as demographic characteristics, political preferences and beliefs, finances, health conditions, browsing activity, shopping habits, travel activities, digital identifiers, geolocation signals, employment information, and more—and then widely share that data with potential advertisers in, essentially, algorithmic online auction houses;[3]
- *Smartphones* that people carry on their person near-constantly and that collect and frequently transmit (including, in some cases, directly and indirectly to data brokers and RTB networks) data such as texts, emails, phone calls, video calls, information on apps installed on a device, information on usage of those apps, web browsing data, face images, voice recordings, contact lists, 24/7 phone geolocation signals, and much more;
- *Wearable devices* such as fitness trackers that collect and potentially share biometric information, biophysical data and signatures, geolocation signals, and much more;
- *Vehicles* that increasingly collect and transmit (including, in some cases, directly and indirectly to data brokers and RTB networks) telemetry such as the dates and times of trips taken, how hard a driver brakes, how hard a driver turns a wheel, how fast a driver drives, the geolocations of their trip visits, and more;[4]

---

[1] For some history in this area, see, for instance: Ludo Block, "The long history of OSINT," *Journal of Intelligence History* 23, no. 2 (2024): 95-109, https://www.tandfonline.com/doi/full/10.1080/16161262.2023.2224091.

[2] Pam Dixon. Testimony before the Senate Committee on Commerce, Science, and Transportation. Hearing on "What Information Do Data Brokers Have on Consumers, and How Do They Use It?," World Privacy Forum, December 18, 2013. https://worldprivacyforum.org/documents/124/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf; U.S. Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability: A Report of the Federal Trade Commission*. Washington, D.C.: Federal Trade Commission, May 2014. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (Durham: Duke University, August 2021), https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/.

[3] Sara Geoghegan, "What is Real Time Bidding?," Electronic Privacy Information Center, January 15, 2025, https://epic.org/what-is-real-time-bidding/.

[4] Vehicles also come with a wide range of potential software and hardware plugins, and many insurance and other companies (like emergency response service vendors) offer small boxes that can be put in a vehicle and transmit data (including geolocation) as well. See, for instance, Jen Caltrider, Misha Rykov, and Zoë MacDonald, "It's

- *Internet and digital networks*, including future generations of ever-"smarter" telecommunications networks, that collect and transmit tremendous amounts of data on individual devices and device users—including persistent digital identifiers and other forms of "digital exhaust" that can be used to create mosaic profiles on individuals, pulling in disparate data from different online browsing sessions, devices in use, and so forth—as well as enable connectivity between ever-more digital devices and other systems, including smartphones, wearable devices, and vehicles; and, among many others,
- *Commercial data analytic capabilities* that enable relatively cheap, sometimes automated, typically scalable, and quite effective means of aggregating, filtering, repackaging, analyzing, and reidentifying datasets—a phenomenon further accelerated by artificial intelligence (AI) and machine learning (ML) technologies—including to identify patterns, flag anomalies, make future predictions, pair up disparate and apparently disconnected pieces of information, uncover the identities of individuals represented in datasets whose identities are supposed to be masked, identify people using facial and voice recognition, and link wide-ranging sets of data to specific individuals and their various identifiers.

This has afforded the U.S. government a number of opportunities and potential advantages in military and intelligence operations. For example, when the internet globally exploded, it prompted much discussion about the implications for U.S. intelligence and security.[5] The Defense Department ordered the creation of U.S. Cyber Command (CYBERCOM) in 2009 out of recognition of the importance and vulnerability of computers and networks in the United States and globally, "creating global networks and allowing adversaries to access strategic centers of national power."[6] More recently, the previous Director of the CIA stated that OSINT plays a "critical role" in "defending our country and values."[7] The intelligence community's 2024-2026 OSINT strategy declared that "OSINT both enables other intelligence collection disciplines and delivers unique intelligence value of its own, allowing the IC to more efficiently and effectively leverage its exquisite collection capabilities."[8] The intelligence community's OSINT Executive said in December 2024 that OSINT "provides at least 20% of all citations in the President's Daily Brief."[9] Discussions about digital connectivity, commercial data, and much more continue, too.[10]

Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy," Mozilla Foundation, September 6, 2023, https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/; U.S. Federal Trade Commission, "FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent," FTC.gov, January 16, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data.

[5] A. Denis Clift, "Intelligence in the Internet Era," *Studies in Intelligence* 47, no. 3 (2003), https://www.cia.gov/resources/csi/static/Intel-in-Internet-Era.pdf.

[6] U.S. Cyber Command, "Our History," cybercom.mil, accessed October 4, 2025, https://www.cybercom.mil/About/History/.

[7] U.S. Office of the Director of National Intelligence, "ODNI and CIA Release the Intelligence Community OSINT Strategy for 2024-2026," DNI.gov, March 8, 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3784-odni-and-cia-release-the-intelligence-community-osint-strategy-for-2024-2026.

[8] U.S. Office of the Director of National Intelligence. *The IC OSINT Strategy 2024-2026*. Washington, D.C.: Office of the Director of National Intelligence, March 2024. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf. 2.

[9] "Re-post of Awards Reception Keynote Speaker Jason Barrett," OSINTFoundation.com, December 30, 2024, https://www.osintfoundation.com/NewsBot.asp?MODE=VIEW&ID=30962.

[10] "Commercially Available Information," intelligence.gov, accessed October 4, 2025, https://www.intelligence.gov/commercially-available-information.

Simultaneously, the United States is unfortunately behind in recognizing the threats all this information, data, and connectivity poses to national security—including U.S. military servicemembers and all other Americans who serve our country, from diplomats to intelligence community personnel to contractors in the scientific and defense industrial base.[11] Each of these categories above clearly or likely exposes data on U.S. military servicemembers, other U.S. government national security personnel, U.S. military and government activities in the national security realm, and, among others, U.S. military and government facilities. Examples include:

- *Open-source information:* "We see the Chinese intelligence officers using social media platforms to reach out to people," a then-official at the Department of Justice's National Security Division told the media in 2019, in reference to Chinese government espionage efforts to identify Americans from whom it wants to extract information.[12] "We've seen China's intelligence services doing this on a mass scale," the then-director of the National Counterintelligence and Security Center added.[13]
- *Commercial data*: I designed and ran a Defense Department-funded, unclassified academic threat assessment looking at the commercial data and data brokerage ecosystem to evaluate the targeting packages that a foreign adversary could assemble based on buying data about U.S. military personnel from U.S. data brokers. We set up a U.S.-based *.org* and a Singapore-based *.asia* website, contacted several U.S. data brokers, and managed to buy individually identified, sensitive contact, financial, health, and other data on thousands of active-duty U.S. military servicemembers, with virtually no serious background checks or vetting, for as little as $0.12 per servicemember—even successfully geofencing some of the data to bases publicly known to house active-duty U.S. special forces operators. The data brokers in question apparently had no issue sending the data overseas, either.[14]
- *RTB networks:* An analysis of RTB segments identified data available on the market that was pointing to people working in the aerospace and defense sector, individuals working in sensitive industries such as nuclear energy and space technology, people who had visited security conferences, individuals within six miles of a military base, and, among others, datasets titled "People who work in the Pentagon," "Department of Defense," "People working in defense & space," and "People who work in the military" as well as individuals categorized as "Government – Intelligence and Counterterrorism."[15]
- *Smartphones:* More than 3 billion phone location pings made available by a U.S. data broker, which were reportedly originally gathered and shared by a Lithuanian data broker, showed phones traveling from U.S. military barracks in Germany to work buildings, Italian

[11] To be clear, this data and digital connectivity explosion threatens the privacy of all Americans, too, including for people who do not and never will work in public service—even if the impacts on different people, such as those who do serve in the national security community, may land in different ways in different contexts.
[12] Ryan Lucas, "People Are Looking At Your LinkedIn Profile. They Might Be Chinese Spies," NPR, September 19, 2019, https://www.npr.org/2019/09/19/761962531/people-are-looking-at-your-linkedin-profile-they-might-be-chinese-spies.
[13] Edward Wong, "How China Uses LinkedIn to Recruit Spies Abroad," *The New York Times*, August 27, 2019, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.
[14] Justin Sherman et al., *Data Brokers and Sensitive Data on U.S. Individuals* (Durham: Duke University, November 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.
[15] Johnny Ryan and Wolfie Christl, *America's Hidden Security Crisis: How Data About United States Defence Personnel and Political Leaders Flows to Foreign States and Non-State Actors* (Dublin: Irish Council for Civil Liberties, November 2023), https://www.iccl.ie/digital-data/americas-hidden-security-crisis/, 12.

restaurants, grocery stores, and bars. The data showed 189 devices moving around inside a high-security German military installation, up to 1,257 devices at Grafenwöhr Training Area where thousands of U.S. troops are stationed, and even four mobile devices traveling from Ramstein Air Base to off-base brothels.[16]

- *Wearable devices:* A wearable device-linked software application, Strava, which people use to track their runs, was around 2018 apparently exposing many users' location histories—their logged movements around the world—on a publicly viewable website. Researchers were able to use the data to track what appeared to be various government personnel all around the world, including what appeared to be active-duty U.S. military servicemembers jogging and moving around forward operating bases in Afghanistan.[17]
- *Vehicles:* General Motors and OnStar allegedly collected, used, and sold drivers' precise geolocation data and driving behavior data from millions of vehicles—including the collection of precise geolocation data from millions of Gen10+ OnStar vehicles every three seconds from the moment of ignition.[18] The data had latitude and longitude points intended to be precise up to six decimal places, which could allegedly pinpoint location accuracy up to 4.5 inches, alongside data on vehicle elevation, heading, current speed, and the date and time for a particular location ping, plus a trip identifier to tie together the route taken by any one vehicle.[19] It speaks to concerns articulated about the national security risks of vehicle data, including when the scenario in question involves Chinese components.[20]
- *Internet and digital networks:* A 2025 report published by the Department of Justice (DOJ)'s Office of the Inspector General (OIG) stated that in 2018, while the FBI was working the drug cartel case against "El Chapo," someone contacted the FBI stating that the cartel had "hired a 'hacker' who offered a menu of services related to exploiting mobile phones and other electronic devices." According to this person, the report detailed, "the hacker had observed people going in and out of the United States Embassy in Mexico City and identified 'people of interest' for the cartel, including the FBI Assistant Legal Attaché (ALAT), and then was able to use the ALAT's phone number to obtain calls made and received, as well as geolocation data, associated with the ALAT's phone." The FBI said, "the hacker also used Mexico City's camera system to follow the ALAT through the city

---

[16] Dhruv Mehrotra and Dell Cameron, "Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany," *WIRED*, November 19, 2024, https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/; Joseph Cox and Dhruv Mehrotra, "The Murky Ad-Tech World Powering Surveillance of US Military Personnel," 404 Media, February 11, 2025, https://www.404media.co/eskimi-2/.

[17] Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases," *The Guardian*, January 28, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[18] U.S. Federal Trade Commission, "FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent"; Federal Trade Commission Complaint in the Matter of General Motors LLC, General Motors Holdings LLC, and OnStar LLC. January 16, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/242_3052_-_general_motors_complaint.pdf. 6.

[19] Federal Trade Commission Complaint in the Matter of General Motors LLC, General Motors Holdings LLC, and OnStar LLC. 6.

[20] See, for instance, Dan Bell, "Modern Vehicles Present Unique Threats and Vulnerabilities to the Military," *Proceedings* 148 (February 2022), https://www.usni.org/magazines/proceedings/2022/february/modern-vehicles-present-unique-threats-and-vulnerabilities; U.S. Bureau of Industry and Security, "Connected Vehicles," BIS.gov, accessed October 4, 2025, https://www.bis.gov/connected-vehicles.

and identify people the ALAT met with," and then intimidated and in some cases killed potential sources or cooperating witnesses against the cartel.[21]

- *Commercial data analytic capabilities:* The *Wall Street Journal* reported in December 2023 that U.S. officials were worried about China using AI capabilities to analyze vast troves of data it stole in hacks of U.S. targets—as well as data on the United States it could further stockpile by using AI technologies—to locate patterns in the data it could use for intelligence advantages and other activities against the United States.[22]

This all creates or exacerbates many risks for the U.S. military and national security community broadly. Data such as device identifiers could be used to persistently track individuals across online and physical spaces, including for reidentifying individuals in datasets that were leaked in criminal data breaches or stolen in cyber espionage campaigns. Foreign adversaries could use this information to target cyber, information, and intelligence operations. Information about health conditions, political preferences and beliefs, shopping habits, degrees of contact with different friends and family members, and more could be used to create profiles of key U.S. negotiators, military leaders, or national security decision-makers. Photos revealing troops on deployment, individuals who apparently know one another, and, in the background, government facilities, equipment, vehicles, military kit, and more could be used to track specific entities overseas, trace connections between individuals, reveal sensitive information about military capabilities and activities, and more. Particularly embarrassing or stigmatized information, such as information indicating infidelity (e.g., the Ashley Madison data hacked and leaked on the web), stigmatized mental health conditions (e.g., in prescription data available from data brokers), or pornographic consumption (e.g., tracked by web analytics technologies as a person browses the internet), could be used for blackmail and coercion of U.S. national security personnel. This illustrative list of potential ways that data and digital connectivity could be exploited could go on and on.

Geolocation data is particularly dangerous. Data capturing the locations of phones, vehicles, and other devices—including location data transmitted via RTB networks and amassed at extraordinary scale for sale by underregulated data brokers—can enable the acquirer of said data to monitor someone's 24/7 movements, build patterns of life, map when two particular devices are near each other or coming into direct contact, and even uncover additional information about those individuals, such as based on visits to government buildings, health clinics, financial offices, political events, gay bars, and much more (even, evidently, brothels). The holder of such location data could also analyze it with the aim of identifying anomalous behavior in device movement patterns, changes in volumes of activity into and out of particular buildings, and so forth. Device-level precise geolocation data, as I have testified and written about before,[23] cannot be

---

[21] U.S. Department of Justice Office of the Inspector General. *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*. Washington, D.C.: Department of Justice Office of the Inspector General, June 2025. https://web.archive.org/web/20250627092903/https://oig.justice.gov/reports/audit-federal-bureau-investigations-efforts-mitigate-effects-ubiquitous-technical. 2.

[22] Robert McMillan, Dustin Volz, and Aruna Viswanatha, "China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says," *The Wall Street Journal*, December 25, 2023, https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594.

[23] See, for instance, Justin Sherman, "Tackling Data Brokerage Threats to American National Security," *Lawfare*, November 25, 2024, https://www.lawfaremedia.org/article/tackling-data-brokerage-threats-to-american-national-security; Justin Sherman. Testimony before the U.S. House Committee on Energy and Commerce: Subcommittee on Oversight and Investigations. Hearing on "Who is Selling Your Data: A Critical Examination of the Role of Data

meaningfully anonymized while preserving any degree of utility to the degree that, say, a company might want, making many claims out in the world about "anonymized" location data fanciful.

All told, there are many risks in this area to Defense Department personnel, Defense Department activities and locations, and the U.S. national security community and U.S. national security broadly—spanning cyber operations, counterintelligence threats, malign information targeting, data analysis and reidentification, anomalous behavior identification, and, among others, profiling individuals, sites, activities, and capabilities.

Brokers in the Digital Economy." April 19, 2023.
https://www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf.

Foreign Adversaries and the Ubiquitous Technical Surveillance (UTS) Environment

The U.S. government has come to use a certain phrase to describe this environment in which U.S. personnel, such as military servicemembers, abroad-stationed law enforcement officers, and members of the intelligence community, must operate: ubiquitous technical surveillance (UTS).

The FBI defines UTS as "the widespread collection of data and analytic methodologies for the purpose of connecting people to things, events, or locations."[24] It notes that while "the risks posed by UTS to the FBI's criminal and national security operations have been longstanding, recent advances in commercially available technologies have made it easier than ever for less-sophisticated nations and criminal enterprises to identify and exploit vulnerabilities created by UTS." Some within the CIA have described the UTS threat as "existential."[25] Then-CIA Director William Burns said in an April 2022 speech at Georgia Tech that UTS "means that intelligence officers are being watched, tracked, and observed all the time. … [T]his has prompted us to fundamentally rethink how we do our operations."[26] A September 2022 Government Accountability Office (GAO) report on the information environment and the Defense Department wrote that because "modern devices, systems, and locations generate, retain, and share enormous volumes of data for broader use," data such as servicemembers' online purchases and information collected from Defense Department weapons platforms "can be collected and shared publicly or can be acquired from data brokers," which poses risks to, or of, force protection, operations security, the safety and security of people's family members, remote surveillance, and intelligence collection.[27]

As an illustration, the GAO report listed several ways that ubiquitous public information could potentially foreshadow a military deployment:

- Social media, traffic applications, and other phone tracking with proximity notifications;
- Hometown school announces plan to create patriotic signs to show their support for departing soldiers;
- Commercial satellite imagery;
- Social media activity and sudden inactivity;
- Hometown news covers reserve transport units activating;
- Contract awarded for logistics services in deployed locations announced;
- Local paper announces arrival of unit for Mission Readiness Exercise;
- Global media depicts U.S. and partner forces building up; and
- Local foreign citizens observe activity and spread information, and social media traffic trends high.[28]

---

[24] U.S. Department of Justice Office of the Inspector General. *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*. i.
[25] Ibid.
[26] William Burns, "The Role of Intelligence at a Transformational Moment," Speech at Georgia Tech, April 14, 2022, https://www.cia.gov/static/Director-Burns-Speech-and-QA-Georgia-Tech.pdf, 6.
[27] U.S. Government Accountability Office. *Information Environment: Opportunities and Threats to DOD's National Security Mission*. GAO-22-104714. Washington, D.C.: Government Accountability Office, September 2022. https://www.gao.gov/products/gao-22-104714. 6.
[28] Ibid.

A 2023 MITRE report surveying commercial advertising technologies' intelligence and national security risks to the United States noted that "many national policymakers still do not fully appreciate the overarching national security considerations of commercial surveillance technology that continuously collects personal information, ostensibly to better tune advertising." It cataloged at least several ways these commercial capabilities could be leveraged against the United States and its interests:

- Targeting individuals for blackmail and coercion;
- Physically mapping and targeting sensitive sites, security measures, high-risk personnel, and operations;
- Creating near real-time situational awareness of U.S. soft targets; and
- Targeting offensive cyber operations and network exploitation.[29]

A 2023 book chapter on UTS noted that "UTS affects all tradecraft—technical, operational, and administrative—in every contested physical, technical, and cyber domain."[30] An article posted on the U.S. Army website wrote that the "constant monitoring" inherent to UTS "allows for the long-term storage and analysis of information, potentially reconstructing past events indefinitely."[31] All these discussions speak to the above explosion of data and digital connectivity in the last two decades. Whether UTS is the ideal term or not, it does appear to attempt to capture everything from how open-source websites could be monitored, commercial data about organizations could be purchased, and digital exhaust about individuals could be picked up from advertising systems to how a government could set up networks of AI facial recognition-powered CCTV cameras, Internet of Things (IoT) sensor networks, and other digital surveillance capabilities to monitor people as they move around the world and within that government's own borders.

The United States' foreign adversaries, such as China and Russia, are investing readily to be able to exploit these vulnerabilities across the explosion of data and digital connectivity—and to leverage commercial data analytic capabilities and more to their own advantages. A January 2022 report from a senior advisory group panel at the Office of the Director of National Intelligence, which was subsequently declassified and published, noted that commercially available information "raises counter-intelligence risks for the IC" and the information is also available to foreign adversaries and "offers [them] intelligence benefits."[32]

---

[29] Kirsten Hazelrig, *Surveillance Technologies Are Imbedded Into the Fabric of Modern Life—The Intelligence Community Must Respond* (McLean: MITRE, January 2023), https://www.mitre.org/sites/default/files/2025-01/PR-22-4107-Surveillance-Technologies-Are-Imbedded-25.pdf, 1.
[30] Craig W. Gruber et al., "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue," in *Fostering Innovation in the Intelligence Community: Scientifically-Informed Solutions to Combat a Dynamic Threat Environment* (New York: Springer, 2023), ed. Craig W. Gruber and Benjamin Trachik.
[31] Ma'Ceo Bell, "Data Security Concerns Rise as Surveillance Becomes Ubiquitous," army.mil, August 12, 2025, https://www.army.mil/article/287760/data_security_concerns_rise_as_surveillance_becomes_ubiquitous.
[32] U.S. Office of the Director of National Intelligence. *Senior Advisory Group Panel on Commercially Available Information*. Washington, D.C.: Office of the Director of National Intelligence, January 2022 (declassified and published June 2023). https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf. 7.

China. The Chinese government "has embarked on an ambitious national data strategy with the goal of acquiring, controlling, and extracting value from large volumes of data."[33] This spans various strategic, legal, and policy efforts to build out structures to accelerate the collection and use of data for national objectives, including AI research and development.[34] Many examples of specific risk activities abound. For instance, the Chinese government has stolen massive troves of data from the United States in the last decade-plus, such as in breaches of data broker Equifax, the Office of Personnel Management (OPM), Marriott, and more; these are the kinds of troves of data that could be combined and analyzed with commercial data analytic capabilities to identify patterns in travel or other behavior, build profiles on U.S. government personnel, target future cyber operations, train AI models to make predictions on particular subjects, and so forth. *Foreign Policy* reported in 2020 that the Chinese government used stolen data to expose CIA operatives in Africa and Europe.[35] Alongside hacks, there are private firms in China offering up OSINT collection capabilities: Shenzhen Zhenhua Data Technology, a small Chinese company, was seemingly collecting millions of social media data points on "foreign political, military and business figures, details about countries' infrastructure and military deployments, and public opinion analysis." The database reportedly had information "on more than 2 million people, including at least 50,000 Americans."[36]

And Beijing can leverage the data and digital explosion against the United States, U.S. military servicemembers, and others serving in the U.S. national security community in other ways. One report claims that China has AI software to recognize faces and detect the gait of individuals, such as American spies.[37] Another examines how China's People's Liberation Army (PLA) is using new collection, processing, and analysis technologies to exploit open-source information and other data sources to monitor government agencies, think tanks, militaries, universities, defense industry companies, scientific research organizations, individuals, and more in the United States and other

---

[33] Samm Sacks. Testimony before the U.S. Senate Committee on Finance: Subcommittee on Fiscal Responsibility and Economic Growth: Subcommittee on Fiscal Responsibility and Economic Growth. Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector." December 7, 2021. https://www.finance.senate.gov/imo/media/doc/Samm%20Sacks%20Testimony%20-%20Senate%20Finance%20-%20December%207%202021.pdf. 1.

[34] See, for instance, among many other readings around this topic, Matthew Johnson, *China's Grand Strategy for Global Data Dominance* (Stanford: Hoover Institution, April 2023), https://www.hoover.org/research/chinas-grand-strategy-global-data-dominance; Kendra Schaefer, "Seeking the next DeepSeek: What China's generative AI registration data can tell us about China's AI competitiveness," Trivium China, April 29, 2025, https://triviumchina.com/research/seeking-the-next-deepseek-what-chinas-generative-ai-registration-data-can-tell-us-about-chinas-ai-competitiveness/; Rogier Creemers, "China's emerging data protection framework," *Journal of Cybersecurity* 8, no. 1 (2022), https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794; Nicole Sganga, "Chinese hackers took trillions in intellectual property from about 30 multinational companies," CBS News, May 4, 2022, https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/.

[35] Zach Dorfman, "China Used Stolen Data to Expose CIA Operatives in Africa and Europe," *Foreign Policy*, December 21, 2020, https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

[36] Gerry Shih, "Chinese firm harvests social media posts, data of prominent Americans and military," *The Washington Post*, September 14, 2020, https://www.washingtonpost.com/world/asia_pacific/chinese-firm-harvests-social-media-posts-data-of-prominent-americans-and-military/2020/09/14/b1f697ee-f311-11ea-8025-5d3489768ac8_story.html.

[37] Julian E. Barnes and Edward Wong, "In Risky Hunt for Secrets, U.S. and China Expand Global Spy Operations," *The New York Times*, September 17, 2023, https://www.nytimes.com/2023/09/17/us/politics/us-china-global-spy-operations.html.

countries. The report identified specific PLA interest in OSINT about subjects such as U.S. military distributed ground intelligence equipment, U.S. main battle tanks, U.S. armored equipment, and the U.S. Marine Corps' operational concepts and equipment.[38] Because of the sizes and lack of regulation of the U.S. data brokerage ecosystem and the U.S. digital advertising ecosystem, there is also a risk of Chinese entities establishing front companies to purchase sensitive data from U.S. data brokers or otherwise extracting it from ad networks.[39]

Domestically (in China), the Chinese government also has a massive digital surveillance apparatus, including architectural-level control of internet infrastructure and routing protocols, data interception and intelligence access laws,[40] sophisticated facial recognition systems paired up to CCTV networks,[41] voice recognition technology for phone calls,[42] and much more. This enables or exacerbates human rights violations[43] and can also pose risks to U.S. national security. For instance, a former CIA officer who served as the Agency's first chief of tradecraft and operational technology said earlier this year, as paraphrased by *The Washington Post*, that "a hostile intelligence service such as China's could discover days, or even months, later that a traitor in its ranks had met with a CIA officer by running big data feeds from cameras across the country through sophisticated artificial intelligence filters."[44]

Russia. The Russian government maintains robust cyber and intelligence capabilities that can be applied for tasks such as exploitation of mobile devices, breaching critical infrastructure systems with sensitive data, and much more to further Russia's information and intelligence objectives.[45] Russian military and intelligence contractors in the private sector are constantly refining their OSINT and data collection tradecraft, including lately with questions around how to use AI and

---

[38] *Private Eyes: China's Embrace of Open-Source Military Intelligence* (Somerville: Recorded Future, June 2023), https://www.recordedfuture.com/research/private-eyes-chinas-embrace-open-source-military-intelligence.
[39] See, for instance, Justin Sherman, "Data Brokerage and the Third-Country National Security Problem," *Lawfare*, April 16, 2025, https://www.lawfaremedia.org/article/data-brokerage-and-the-third-country-national-security-problem.
[40] *China's National Security Laws: Implications Beyond Borders* (Arlington: Center for Naval Analyses, December 2023), https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf.
[41] Dave Davies, "Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State,'" NPR, January 5, 2021, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta.
[42] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (January 2019): 53-67, https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/.
[43] Johana Bhuiyan, "'There's cameras everywhere': testimonies detail far-reaching surveillance of Uyghurs in China," *The Guardian*, September 30, 2021, https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china; Dake Kang and Yael Grauer, "Silicon Valley enabled brutal mass detention and surveillance in China, internal documents show," Associated Press, September 9, 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dadb6aea230f18170ed54e88.
[44] Warren P. Strobel and Ellen Nakashima, "CIA chief faces stiff test in bed to revitalize human spying," *The Washington Post*, May 28, 2025, https://www.washingtonpost.com/national-security/2025/05/28/cia-spy-china-russia-ratcliffe/.
[45] UK National Cyber Security Centre, "Case study: Russia," NCSC.gov.uk, 2023, https://www.ncsc.gov.uk/collection/annual-review-2023/threats-risks/case-study-russia; Andrei Soldatov and Irina Borogan, *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities* (Washington, D.C.: Center for European Policy Analysis, September 2022), https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

ML technologies.[46] The Russian state, like many other adversaries and competitors of the United States, has also been increasing its investments in AI research and development for military purposes[47] (although, like much else in Russia's tech sphere, the results remain to be seen).

Domestically (in Russia), the Russian government's surveillance infrastructure is also expanding. The Federal Security Service (FSB) operates SORM-3, Russia's surveillance system for intercepting and storing digital traffic. Authorities are currently pushing out, including through coercive measures, a "super app" that would greatly expand the state's surveillance to devices throughout the country.[48] During the Covid-19 lockdown, Russia upped its use of AI facial recognition on cameras in major cities such as Moscow.[49] Recently, the Russian government has started deploying biometric surveillance systems at a limited number of border crossings and airports with the intent to expand the system to all border crossings and airports into Russia.[50]

Other countries can exploit the data and digital connectivity explosion as well. For example, threat actors in Iran and North Korea are already using large language models developed by U.S. companies to conduct open-source research against what can be assumed to be potential U.S. targets for cyber or other operations.[51]

---

[46] Witness' open-source research.
[47] Sergey Sukhankin, "Russia Capitalizes on Development of Artificial Intelligence in Its Military Strategy," *Eurasia Daily Monitor* 22, no. 27 (March 2025), https://jamestown.org/program/russia-capitalizes-on-development-of-artificial-intelligence-in-its-military-strategy/.
[48] Ksenia Elzes, "Everything You Need to Know About Max, Russia's State-Backed Answer to WhatsApp," *The Guardian*, August 28, 2025, https://www.themoscowtimes.com/2025/08/28/everything-you-need-to-know-about-max-russias-state-backed-answer-to-whatsapp-a90356; forthcoming article by witness.
[49] Patrick Reevell, "How Russia is using facial recognition to police its coronavirus lockdown," ABC News, April 30, 2020, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736.
[50] Justin Sherman, "Russia Is Bringing Biometric Surveillance to a New Level," *Barron's*, January 2, 2025, https://www.barrons.com/articles/russia-biometric-surveillance-face-scan-airport-f428a10e?st=1HprPL. See also: RFE/RL's Central Asian Migrants' Unit, RFE/RL's Russian Service, and Ajla Obradovic, "Russia's Migrant Crackdown Expands With Mandatory Mobile Tracking," RadioFreeEurope/RadioLiberty, June 6, 2025, https://www.rferl.org/a/surveillance-migrant-workers-moscow-central-asia-visa/33433055.html.
[51] "Disrupting malicious uses of AI by state-affiliated threat actors," OpenAI.com, February 14, 2024, https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/.

Mitigation Discussions

Given the threats, there are growing discussions about potential ways for the U.S. government to better mitigate UTS and better protect the data—and, ultimately, safety and security—of U.S. national security personnel, the government, and the country itself.

- A June 2024 MITRE report wrote that the term UTS describes the surveillance environment but does not adequately describe per se what individuals, groups, businesses, or states can do with the data gathered from the UTS environment. It encouraged a discussion about the later "PED" part of the "TCPED" intelligence cycle in the context of adversaries' UTS capabilities—that is, thinking not just about foreign adversaries' Tasking and Collection in the UTS context, but what their Processing, Exploitation, and Dissemination capabilities might look like—to "conceptualize adversarial capabilities along the spectrum of data analysis and data science processes, with or without augmentation by AI."[52]
- A number of companies publicly advertise capabilities to protect the privacy and security of devices, networks, individuals whose data is gathered and sold, and so on.
- A 2023 report from the Army Cyber Institute suggested various UTS mitigations spanning steps that are technical (e.g., provide servicemembers with privacy protective services), policy-related (e.g., better communicate the risks of publicly and commercially available data to policymakers), doctrinal (e.g., integrate commercial and publicly available information risk management in key organizational policies and doctrines), personnel-related (e.g., dedicate red teams to assess friendly signatures created by personnel and operations), contracting-related (e.g., include privacy-enhancing requirements in contracts to deal with issues such as telemetry leakage and data sales), and awareness- and training-related (e.g., research and maintain context-specific mitigation guides).[53]
- The 2025 DOJ OIG report mentioned above recommended that the FBI—which could be modeled in other agencies—thoroughly document and incorporate all identified UTS vulnerabilities into its final UTS mitigation plan; finalize its UTS strategic plan, including to appropriately leverage existing resources and to ensure FBI officials with the authority to execute are properly identified and empowered; establish a clear line of authority for responding to enterprise-wide, UTS-related incidents; and assess its ability to further expand the availability of its advanced UTS-related training modules and take necessary steps to ensure personnel are adequately trained on both basic and advanced mitigations.[54]

---

[52] Shawn Benson, *Deciphering Ubiquitous Technical Surveillance with Data-Driven Analytics and Artificial Intelligence* (McLean: MITRE, June 2024), https://www.mitre.org/news-insights/publication/deciphering-ubiquitous-technical-surveillance, 2-3.
[53] Jaclyn Fox et al., *Death by a Thousand Cuts: Commercial Data Risks to the Army* (West Point: Army Cyber Institute, 2023), https://cyber.army.mil/Portals/3/Documents/2023_ACI_Commercial_Data_Report.pdf, 15-17.
[54] U.S. Department of Justice Office of the Inspector General. *Audit of the Federal Bureau of Investigation's Efforts to Mitigate the Effects of Ubiquitous Technical Surveillance*. 14.

Steps Congress Can Take Now

There are three steps Congress can take now:

1. At the operational level, Congress should compel the defense community to thoroughly evaluate critical UTS mitigation gaps across and between agencies. The UTS environment and foreign adversaries' investments in exploiting it are continuously evolving anyway, and the 2025 DOJ OIG report made clear that the FBI may have additionally insufficient policies and practices to mitigate the risks to its mission and personnel. Some experts have already put forward hypotheses as to what might explain gaps between the FBI's UTS-mitigation efforts to date and those of other agencies.[55] This same issue set is worth examining within and across the Defense Department, including enterprise-wide and within and between constituent agencies and elements. For example, the Department responded to the 2018 Strava location data scandal by issuing a policy that prohibited the use of geolocation features and functionality on both non-government and government-issued devices, applications, and services while in locations designated as operational areas.[56] While an important step, this response has been wholly inadequate to deal with other, similar ways that location data is gathered on U.S. military servicemembers on and/or around U.S. military sites.[57] Years into that 2018 Department policy, location data around military sites and potentially on military servicemembers' devices is widely available on the commercial market, as further clarified when a data broker offered to sell such data to my team when I was running the aforementioned Defense Department-funded threat assessment on brokered data. The Committee and the Subcommittee should work with the defense community to ensure the Department is assessing what critical gaps might exist in efforts to mitigate UTS threats in specific agencies and in the overall community, to include potentially requiring the Department to generate a report like the one the DOJ OIG produced on the FBI's UTS mitigations. The Committee and Subcommittee could additionally require the Department (e.g., in oversight requests or future legislative language) to provide closed, secure briefings to the relevant committees on the findings—as well as wider briefings or hearings when information can be more widely shared—to advance a better understanding of the digital threat environment, ways the United States can seek advantage, and what U.S. risk mitigations and countermeasures are needed to protect the military and U.S. national security.
2. At the policy level, Congress should add language into the National Defense Authorization Act (NDAA) to lock down Americans' data and shift some of the surveillance-prevention burden off national security personnel. Building on recent efforts such as E.O. 14117 and the resulting Department of Justice bulk data transfer/data brokerage and national security

[55] Susan Landau, "The FBI's Dangerous Failure to Adapt to the Digital Age," *Lawfare*, July 7, 2025, https://www.lawfaremedia.org/article/the-fbi-s-dangerous-failure-to-adapt-to-the-digital-age.
[56] Department of Defense. Memorandum on Use of Geolocation-Capable Devices, Applications, and Services. August 3, 2018. https://media.defense.gov/2018/Aug/06/2001951064/-1/-1/1/GEOLOCATION-DEVICES-APPLICATIONS-SERVICES.PDF.
[57] See, for instance, Byron Tau, "The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots," *The Wall Street Journal*, April 26, 2021, https://www.wsj.com/tech/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402.

program,[58] the bipartisan Protecting Americans' Data from Foreign Adversaries Act (PADFAA),[59] and some amendments made in recent years' NDAAs, the Committee and the Subcommittee should include language in upcoming NDAAs that would: fund and compel both open-source/unclassified and classified research into the UTS threat environment and the Defense Department's exposure, diving deep into several, specific dimensions of risk (e.g., commercial data analytic technologies widely available on the commercial market, connected vehicles, commercial advertising networks) as well as investments from adversaries; strengthen language in the Defense Federal Acquisition Regulation Supplement (DFARS) to ensure Defense Department contractors are subject to more rigorous screening and tighter privacy and cybersecurity controls, such as prohibitions on contracting with entities that have unacceptable data security practices and strong restrictions on how any Department contractor can use even unclassified Department and personnel data they obtain in the course of a contract;[60] and propagate data privacy and security protections that are as wide as possible to protect U.S. national security.[61] It is also worth stressing that Congress should pass a strong, comprehensive, federal privacy law to protect all Americans' data. While protections implemented in a consumer context will not be wholly sufficient to mitigate enhanced levels of risk or different kinds of risk to U.S. national security in particular, a broader privacy law—such as one that raises minimum data protection standards for companies, bolsters vehicle privacy, strongly regulates the data brokerage industry, and puts responsible safeguards around commercial advertising networks—could shift some of the risk mitigation burden off U.S. national security personnel and raise the privacy baseline for all Americans.[62] Even data made widely available on civilians and non-defense-affiliated U.S. businesses is of interest to the United States' foreign adversaries, too.

3. At the strategic level, Congress should push the U.S. national security community and policymakers in general to rethink the United States' societal "connect now, assess later" attitude. While this is not meant to suggest that U.S. executive branch or Defense Department agencies are quite literally installing all kinds of technologies without any thought or process, this phrase (and recommendation) is meant to capture, and call for a rethinking of, the United States' trajectory in the past couple of decades. New technologies are built, proliferated, and used typically without much consideration for privacy,

---

[58] Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons. A Rule by the Justice Department. 90 *FR* 1636. January 8, 2025. https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

[59] Protecting Americans' Data from Foreign Adversaries Act. 2024. https://www.congress.gov/bill/118th-congress/house-bill/7520/text.

[60] I of course welcome further conversation with the Committee and the Subcommittee about what those specific measures might look like.

[61] I of course welcome further conversation with the Committee and the Subcommittee about what those specific measures might look like. Recent bills in this area include: "Cassidy, Warren, Rubio Introduce Protecting Military Service Members' Data Act of 2022," Cassidy.senate.gov, May 19, 2022, https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-warren-rubio-introduce-protecting-military-service-members-data-act-of-2022/; "Cassidy Introduced Bill to Further Protect Military Servicemembers' Data," Cassidy.senate.gov, April 29, 2025, https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-introduced-bill-to-further-protect-military-servicemembers-data/.

[62] Justin Sherman, "Ubiquitous Technical Surveillance Demands Broader Data Protections," *Lawfare*, July 25, 2025, https://www.lawfaremedia.org/article/ubiquitous-technical-surveillance-demands-broader-data-protections.

cybersecurity, resilience, and threats to national security at all. There is a general societal attitude that risks from digital technologies can be dealt with later. (This is not entirely the fault of individuals and customers per se and can be attributed in part to corporations that deploy technologies that are poorly designed, are intended to collect vast volumes of data, have not been adequately tested before launch, and so forth.) Designing commercial technologies and not thinking seriously and deeply about their impacts, or thinking all risks can simply be mitigated at the deployment stage (versus, for instance, considering that perhaps some commercial technologies should not be built or widely deployed to begin with), ends up hurting U.S. national security—such as through the explosive growth of open-source information and commercial data available on Americans, including U.S. military servicemembers. This societal trajectory also loses an opportunity: pursuing the design, development, deployment, and evolution of societally valuable, innovative technologies that better protect Americans and the country, including in ways that better protect people's privacy and build towards systemic resilience. Congress should therefore continue to hold hearings on ways to better design, regulate, and deploy technologies to pursue innovation, social benefit, the protection of Americans' rights and freedoms, and the advancement and protection of national security—including the people serving their country in the national security community every single day.

The explosion of data and digital technologies in the last two decades has presented the United States with many potential opportunities to seek advantage. But it has also come with tremendous risk, including to U.S. military servicemembers, the U.S. Defense Department (from operations to capabilities to broader mission), and U.S. national security writ large. Proactive measures to address the current threat environment across law, policy, technology, education, and more—at tactical, operational, and strategic levels—can help to improve on the status quo and better prepare the United States to operate in the increasingly data-heavy, highly digitally connected future.

Chairwoman ERNST. Yes, thank you, Mr. Sherman.
Mr. Doyle, you are recognized.

STATEMENT OF JOHN DOYLE, CHIEF EXECUTIVE OFFICER, CAPE

Mr. DOYLE. Chairwoman Ernst, Ranking Member Slotkin, and Members of the Committee, thank you for the opportunity to appear here today. My name is John Doyle. I am a former U.S. Army Special Forces sergeant and the founder and CEO of Cape.

Cape is a mobile carrier that safeguards user privacy and security by systematically solving the technical vulnerabilities that plague commercial cellular networks. We serve customers within

the government along with commercial enterprise and everyday consumers.

Back in 1991, members of the press were able to predict the timing of Operation Desert Storm due to an unusual lapse in security. They had figured out that late-night pizza deliveries to the Pentagon spiked dramatically when major operations were about to launch. Thirty-five years later, those who wish to suss out sensitive information about troop positions, patrol routes, or the timing of operations no longer need to call Domino's. These days, it is much easier to figure out.

That is because today's military relies heavily on the same commercial cellular networks that we all use every day and the same carriers that are regularly and repeatedly hacked and exploited. These networks are almost universally available, including on the battlefield, making them irresistibly convenient to use in military contexts. This in turn makes it easy for determined actors to track the activity of military personnel based solely on the phones they carry in their pockets and the volumes of data that those phones produce.

The consequences of our reliance on these networks have been felt on the home front, including most recently through the Salt Typhoon cyberattacks, and the battlefield is no different. In Ukraine, both Ukrainian and Russian forces use commercial cellular networks heavily to coordinate operations and carry out intelligence gathering, despite wide reporting that both sides are also targeting each other based on cell phone location data. Ukraine took new advantage of cell network availability this summer with Operation Spiderweb, embedding Subscriber Identifcation Module (SIM) cards into drones and using Russia's own mobile networks to remotely pilot them into Russian targets.

Cell phones are not responsible for 100 percent of the data vulnerabilities that military personnel face, but I would put it close to 85 percent. The well-known and frequently exploited weaknesses of commercial networks, paired with the volume of publicly available data our adversaries can readily access, make it possible to learn far too much about the habits and locations of our servicemembers at scale. Advanced data analytics platforms now allow bad actors to easily correlate information across datasets, making the intelligence value of telecommunications data even more extreme.

Phone carriers abet this State of affairs by monetizing customers' data directly, selling some of the most exquisite pattern-of-life data imaginable to governments and private entities alike. Some applications, some apps, exist to mitigate certain threats at the device and app layer, but before Cape, there was essentially nothing a user could do, even when that user is a national security professional or a servicemember, to mitigate risks at the network level. And if I may, the problem is compounded by bureaucratic processes at the Pentagon that funnel all cellular service procurement to a 10-year Indefinite Delivery, Indefinite Quantity (IDIQ) contract called Spiral 4 that has not been opening onramps to new, innovative entrants since the last award.

Still worse, the contract is written to insist on procurement of lowest-priced, technically acceptable solutions, in other words, buy-

ing cellular service based on price only and not insisting on solutions to the problems inherent in the incumbents. I would be remiss if I didn't specifically mention section 1513 of the House fiscal year 2026 NDAA, which addresses these shortcomings, and I would ask for this body's support of that provision through the conference process.

The threat the status quo poses is profound. Every servicemember has a smartphone in their cargo pocket. The good news is that this is not an intractable problem. My company is just one of several working in the problem space, and others are represented here at the table with me. We at Cape are focused on tackling network vulnerabilities that our adversaries abuse to gain insight into personnel and operations. After decades of stagnation in the security of commercial networks, while technology dedicated to exploiting weaknesses graduated from the Pentagon Pizza Index to state-of-the-art data analytics, we are finally seeing the rise of technology dedicated to fixing those weaknesses instead and traction for policy changes to enable adoption of those technologies by the Force.

Thank you for convening this important conversation, and I look forward to answering your questions.

Chairwoman ERNST. Thank you, Mr. Doyle.

Mr. Stokes, you are recognized for 5 minutes.

STATEMENT OF MICHAEL STOKES, VICE PRESIDENT OF STRATEGY, RIDGELINE INTERNATIONAL

Mr. STOKES. Chair Ernst, Ranking Member Slotkin, and Members of the Subcommittee, thank you for the opportunity to testify.

At Ridgeline, we have followed this problem closely since 2016. In our work across government and industry, we use the term ubiquitous technical surveillance to describe this threat. I will offer two things today, a concise definition of the problem and a path forward.

The Definition. As Mr. Sherman stated, UTS is not just a single sensor you can switch off. It is a fused fabric of phones and apps, connected cars, building cameras, electronic payments, cell and Wi-Fi metadata, plus a vast commercial data market. That fusion exposes patterns, and deviations from those patterns are triggers for an adversary. An unusual no-phone day; synchronized travel by people who should not be connected; a route, flight, or driving pattern that does not match a desired cohort, these anomalies trigger an automated investigation, followed by human scrutiny. Near-peer adversaries and sophisticated non-State actors such as cartels already leverage UTS to anticipate, frustrate, and compromise U.S. missions worldwide.

The Path Out. Admiring the problem is one thing, and this hearing is bringing that right attention to the problem, but awareness without doctrine, policy, standards, and resourcing will not move the needle. At Ridgeline, we enable what we call digital signature warfare, a proactive approach to managing digital signatures so behavior and emissions align with a cohesive cover narrative before, during, and after operations. The aim is simple. Protect the operational act, avoid investigative triggers, and mitigate forensic reconstruction.

So here are four recommendations to make that real. One, name a single accountable lead for UTS and publish an enterprise baseline for signature management. Today, UTS is everyone's problem and no one's priority, so dollars for digital force protection fall below the line. An ad hoc approach to this issue is not sufficient. Task a single office within Office of Secretary of Defense (OSD) of owning the problem. They should issue a digital signature management plan for any device that connects to the public internet. This includes a serious conversation about personal cell phones. This policy should consider commercial data covering device posture, routing diversity, cohort fit, and normalized absence.

Two, protect our people by shrinking the commercial attack surface. The data broker ecosystem still trades in sensitive datasets, including precise geolocation, as we have heard today. Consumer opt-outs will not safeguard a sergeant's commute to base housing, and Congress can direct a department, do not call, collect, or do not sell policy for servicemembers and dependents, enforceable on app stores and brokers with penalties, and require annual inspector general and GAO audits of compliance.

Three, close two infrastructure gaps, telecom and connected vehicles. As the impact of recent Salt Typhoon and recent attacks come into focus, the vulnerabilities of our commercial communications infrastructure are now clearer than ever. This infrastructure compromise illustrates the need for end-to-end encrypted enterprise-grade commercial messaging applications. Connected vehicles are essentially smartphones on wheels equipped with sensors and uplinks. These vehicles feed data into unregulated commercial data economies.

Support the Commerce Department's work to restrict untrusted connected vehicles and fully implement provisions that ban Chinese-connected vehicles on military installations.

Leverage enterprise-grade secure messaging applications, such as Element.io, to communicate unclassified content on phones.

Four, units should deploy a digital mirror, a survey policy, a posture for UTS vulnerabilities, and then adjust routes, timing, and devices' use as they blend into the desired cohort. The objective is not to vanish; it is to look normal, in pattern, all the time.

Effective UTS mitigation is not theoretical. Technology, training, and tradecraft already exist and are being effectively applied at the very peak of our sensitive defense and intelligence operations. It is time to adapt and scale these solutions for a broader force.

Let me close with a family level point. This is not only for soft or intel operators. Spouses, kids, contractors, and base workers all generate these patterns adversaries use. If a hostile actor can determine where a soldier sleeps or where a gate a unit uses, we have ceded initiative. With the steps above, governance, guardrails for commercial data, and infrastructure risk reduction, we can lower trigger rates, make it harder for the enemy to reconstruct an operation, and reduce the cost of secrecy across the force. That is how we turn UTS from a persistent disadvantage into an operational edge.

Thank you for the opportunity to testify.

[The prepared statement of Mr. Michael Stokes follows:]

PREPARED STATEMENT BY MICHAEL STOKES

INTRODUCTION

Chair Ernst, Ranking Member Slotkin, and Members of the Subcommittee, thank you for the opportunity to testify.

My name is Michael Stokes, Vice President of Strategy at Ridgeline International. We have followed this problem closely since 2016. In our work across government and industry, we use the term Ubiquitous Technical Surveillance (UTS) to describe this threat.

I will offer two things today: a concise definition of the problem and a path forward.

The Definition. UTS is not a single sensor you can switch off. It is a fused fabric of phones and apps, connected cars, building cameras, electronic payments, cell and Wi-Fi metadata—plus a vast commercial data market. That fusion exposes patterns, and deviations from those patterns are triggers for an adversary. An unusual no-phone day. Synchronized travel by people who should be unconnected. A route, flight, or driving pattern that does not match the desired cohort. These anomalies trigger an automated investigation, followed by human scrutiny. Near-peer adversaries—and sophisticated non-State actors, such as cartels—already leverage UTS to anticipate, frustrate, and compromise U.S. missions worldwide.

The Path Out. Admiring the problem is one thing; this hearing is bringing the right attention to the problem. But awareness without doctrine, policy, standards, and resourcing will not move the needle. At Ridgeline, we enable Digital Signature Warfare—a proactive approach to managing digital signatures so behavior and emissions align with a cohesive cover narrative before, during, and after operations. The aim is simple: protect the operational act, avoid investigative triggers, and mitigate forensic reconstruction.

Here are Four recommendations to make that real.

One. Name a single accountable lead for UTS and publish an enterprise baseline for signature management.

Today, UTS is everyone's problem and no one's priority, so dollars for digital force protection fall below the line. An ad-hoc approach to this issue is not sufficient. Task a single office in OSD with owning the problem. They should issue a Digital Signature Management plan for any device that connects to the public internet. This includes a serious conversation about personal devices. This policy should consider commercial data, covering device posture, routing diversity, cohort fit, and normalized absence.

Two. Protect our people by shrinking the commercial attack surface.

The data-broker ecosystem still trades in sensitive datasets, including precise geolocation. Consumer opt-outs will not safeguard a sergeant's commute to base housing. Congress can direct a Department "Do-Not-Collect/Do-Not-Sell" policy for servicemembers and dependents—enforceable on app stores and brokers with penalties—and require annual Inspector General and GAO audits of compliance.

Three. Close two infrastructure gaps: telecom and connected vehicles.

As the impact of the recent Salt Typhoon and related attacks comes into focus, the vulnerabilities of our commercial communications infrastructure are now clearer than ever. This infrastructure compromise illustrates the need for end-to-end encrypted enterprise-grade commercial messaging applications. Connected vehicles are essentially smartphones on wheels equipped with sensors and uplinks. These vehicles feed data into unregulated commercial data economies.

Support the Commerce Department's work to restrict untrusted connected vehicles and fully implement provisions that ban Chinese connected vehicles on Military installations. Leverage enterprise-grade secure messaging applications such as Element to communicate unclassified content on phones.

Four. Units should deploy a Digital Mirror, a survey policy, and posture for UTS vulnerabilities, and then adjust routes, timing, and device use until they blend into the desired cohort. The objective is not to vanish; it is to look normal—in pattern—all the time.

CONCLUSION

Effective UTS mitigation is not theoretical. Technology, training, and tradecraft already exist and are being effectively applied at the very peak of our sensitive defense and intelligence operations. It is time to adapt and scale these solutions for the broader force.

Let me close with a family level point. This is not only for SOF or intel operators. Spouses, kids, contractors, and base workers all generate the patterns adversaries use. If a hostile actor can determine where a soldier sleeps or which gate a unit

uses, we have ceded initiative. With the steps above—governance, guardrails for commercial data, and infrastructure risk reduction—we can lower trigger rates, make it harder for the enemy to reconstruct an operation, and reduce the cost of secrecy across the force. That is how we turn UTS from a persistent disadvantage into an operational edge.

Thank you for the opportunity to testify. I look forward to your questions.

[Supporting documentation submitted by Mr. Michael Stokes to follow:]

Obscurity is Dead

Winning in the Age of Ubiquitous Technical Surveillance

Michael Stokes
October 2025

Executive Summary

In 2025, visibility, not obscurity, is the default in modern digital ecosystems; a reality that has made traditional cover harder to sustain, as reported by The Economist's Technology Quarterly. Near-universal device and internet adoption reinforces that baseline. Across government and industry, the Office of the Director of National Intelligence (ODNI) formally recognizes that large pools of commercially available information (CAI) can be acquired and fused for analysis at scale under governance. At the city level, Human Rights Watch has documented how Moscow's facial-recognition network enables real-time identification and retrospective tracing, demonstrating the operational reality of fused surveillance. Even seemingly harmless consumer exhaust can be revealing; WIRED showed how Strava's public heat map illuminated bases and patrol routes, prompting a U.S. military review. To operate effectively in this environment, commanders should adopt Digital Signature Warfare (DSW) – a doctrine that aligns behavior and emissions before, during, and after operations to avoid investigative triggers, protect the operational act, and frustrate forensic reconstruction.

From Sensors to a Fused Data Ecosystem

Ubiquitous Technical Surveillance (UTS) is no longer a single-sensor problem. Data collection is a fused fabric of IoT devices, CCTV/biometrics, telecom metadata, connected-vehicle telemetry, and commercial datasets analyzed at machine scale. Within the U.S. government, the ODNI's 2024 CAI framework codifies how purchasable, sensitive data can be accessed and processed under governance, reflecting the scope and persistence of modern data markets. At the population scale, the Pew Research Center reports that 98% of U.S. adults own a cellphone, and roughly nine in ten own a smartphone, making sustained "no-device/no-signal" behavior unusual in everyday life. China's national initiatives illustrate what fused public-space surveillance looks like at scale: the Sharp Eyes and Skynet programs aim to extend camera coverage across cities and towns and fuse feeds for rapid identification and dispatch. Independent reporting by the UN human-rights office describes intrusive, tech-enabled surveillance as part of wider concerns in Xinjiang, underscoring how data from multiple vectors can be combined for control. Human Rights Watch has reverse-engineered the Xinjiang police "Integrated Joint Operations Platform," showing how authorities flag "abnormal" behavior for investigation – an operational example of anomaly-driven tasking. An Associated Press investigation found that China's predictive-policing and mass-surveillance build-out reinforces how multi-vector data can be combined and weaponized. Beyond China, city networks like Moscow's leverage facial recognition to locate individuals quickly, underscoring that a single break in an established pattern of life can cue automated tasking. In practice, this means a force

can be identified by how its patterns change, through procurement purchases, synchronized travel windows, and out-of-pattern routes, rather than by any single emitter or message.

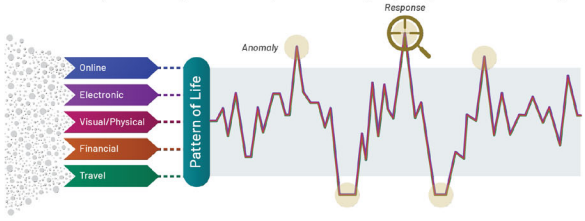


Figure 1. Ridgeline International's Pattern of Life Anomaly Response (POLAR™) Model illustrates the conditions under which deviations from the patterns generated in commercial data can trigger adversary response.

For DoD, the U.S. Army describes UTS as pervasive collection across five vectors: online, financial, electronic, visual, and travel, enabling long-term reconstruction of events.

In Great Power Competition, that five-vector reality changes how we plan and fight. For Large Scale Combat Operations (LSCO), an adversary doesn't need a single perfect intercept; they learn our logistics and movement baselines from ordinary digital exhaust, including fuel and toll records, charter and rail manifests, port and warehouse cameras, fleet telematics, payment cadence, and then alert on deviations that look like mobilization or staging. For supply chains, the same digital fabric can map routes, vendors, and surge timing from freight brokerage data, bills of lading, and facility telemetry. The counter is digital signature shaping at scale – build civilian-cohort noise before you need it, disperse your routes and vendors, time-shift loads, pre-age accounts and devices, and seed decoys so procurements, convoy patterns, and assembly areas read as routine rather than as an anomaly in the data.

For troop movements and Special Operations, Emission Control (EMCON) and "no phone" are necessary but no longer sufficient. Movement is discovered by correlation, not just by communications. The Pentagon Pizza Index is an example of an online tool used to start the investigation. From there, adversaries track data from vehicle telematics, and cell phones around known SOF bases and various public cameras can reveal fleet movement even when radios are quiet.

Why Digital Discipline is Not Enough

Leaving the phone behind used to feel sufficient. Today, it is only the baseline. Re-identification science shows that a few mobility points or attributes can uniquely identify most individuals in large datasets. Platforms in China demonstrate how a single break in routine can cue automated action. The Xinjiang police platform flags "abnormal" device use, movement, or social ties for follow-up. A Justice Department Inspector General audit summarized by Lawfare describes how the Sinaloa cartel mixed phone data with Mexico City cameras to identify and intimidate U.S. contacts – an example of fused replay outside a state surveillance system. Complementary reporting by Homeland Security Today details the "Sinaloa hack of an FBI phone," highlighting operational risks at the edge of fused technical surveillance.

The Salt Typhoon cyberattack compromised the core networks of major telecom and internet service providers, including AT&T, Verizon, and Lumen Technologies. By gaining a foothold in the very systems that route communications, they were positioned to intercept, steal, and surveil data, as well as monitor a vast amount of traffic. This attack proves that even US infrastructure is not impervious to attack and compromise by near peer adversaries.

Third-party exhaust surrounds every mission. Data-broker ecosystems and ad-tech telemetry continue to circulate sensitive location data despite nominal opt-outs, as evidenced by the FTC's case against Kochava and an investigation by WIRED, The Markup, and CalMatters that found dozens of brokers hiding opt-out pages from search.

Complete withdrawal is impractical. Communications, finance, travel, and logistics rely on personal and location data, and both governments and platforms collect this information extensively.

Because commercial data is collected continuously and stored indefinitely, there is a permanent data record of any connection, travel, purchase, or activity. Understanding the full impact of UTS on operations in this fused data ecosystem context requires conceptualizing the operational act in three parts: the act itself; the period to the "left of bang" where research, planning, and preparation take place; and the period to the "right of bang" where adversaries will investigate and act based on forensic clues left at the "X" – the operational site.

When adversaries leverage UTS to create baselines for our data output and flag breaks in our patterns of life, operational success depends less on last-minute evasions or the use of burner phones, than on shaping what the system sees over time. To mitigate these threats, we must avoid investigative triggers before the act, prevent observation during the act, and mitigate forensic reconstruction or attribution once the act has taken place.

New Doctrine: Digital Signature Warfare

Digital Signature Warfare turns your digital signature from a liability into an asset across the full mission timeline, aligning behavior and emissions before, during, and after operations.
DSW executes through four actions:

- **SEE**: using a Digital Mirror to assess discoverability and cohort fit
- **SHAPE**: choosing plausible narratives and measurable shifts
- **CONTROL**: enforcing emissions and behavior that fit those narratives
- **DECEIVE**: misleading adversary models with cover-consistent misdirection

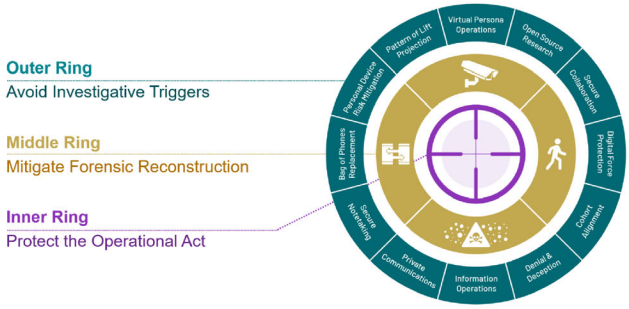


Figure 2: Protecting operations requires confronting UTS threats before, during, and after the operational act by offensively and defensively managing digital signatures.

The Three Rings of UTS Mitigation

These actions, when overlaid on the three-part timeline of an operational act (left of bang, the operational act, right of bang), create a framework for keeping our observable data within pattern to avoid investigative triggers, protect the "X", and mitigate forensic reconstruction.

Outer Ring | Before | Avoid Investigative Triggers: The best outcome is that the adversary never looks. Keep the operator indistinguishable from the cover cohort by maintaining continuity in daily rhythms, venues, and payment patterns, and by avoiding synchronized "dark" windows that deviate from baseline. In a smart city where cameras and data registries are fused, repeated day-long handset silence can act as a soft tag that elevates tasking priority; Chinese

deployments show how fused systems can operationalize such cues at scale. Even though China has signaled that guardrails are needed – its cyberspace regulator issued rules saying facial recognition should not be forced on individuals and must have visible signage – the structural capability remains extensive.

Inner Ring | During | Protect the Operational Act: Do not expose the act. Leave electronics behind, and choose movement that minimizes person/sensor coupling by flowing within cover-cohort pulses and avoiding camera-dense chokepoints.

Middle Ring | After | Mitigate Forensic Reconstruction: Assume the adversary detected that something happened. Deny a clean chain across the five UTS vectors so replay yields ambiguity, not attribution. Police platforms in China demonstrate the replay risk: multi-vector logs – devices, checkpoints, cameras, registries – can be rewound to stitch together people, places, and timelines unless the data yields ambiguity.

A New Approach & Implementation

Because simply leaving phones behind, using burner phones, or practicing good digital discipline are not enough, a new and comprehensive approach is required to maintain our competitive advantage in the UTS environment.

Capabilities without Brands

The point of capability isn't the gear on the table; it's the effect you can deliver in a UTS fight. The disciplines listed below serve as functional building blocks. Used together, they create the outcomes the mission needs over time: avoiding investigative triggers (Outer Ring), protecting the operational act (Inner Ring), and frustrating forensic reconstruction (Middle Ring). Integrated and exercised as a system-of-systems, they let commanders see, shape, control, and deceive what the environment and adversary learn about their force.

Digital Signature Management (Digital Mirror)

A mission-controlled view of the same classes of signals an adversary would use – ad-tech location, mobility traces, building/venue telemetry, and open/closed sources – lets leaders visualize discoverability, run what-if tests, and quantify ambiguity under replay. As a practical benchmark, model Digital Mirrors on the kinds of anomaly flags documented in Xinjiang, and test whether small changes in timing, routes, and device posture suppress or elevate alerts.

Managed Attribution & Device Virtualization

Cover-consistent identities and devices with controllable sensors, plausible account age, and local usage cadence help preserve continuity when the real handset stays behind. Diversified

points-of-presence – residential, commercial, cloud, LTE edges – reduce tie-back and prevent sterile-phone tells.

Secure Mobility Enclaves & Enterprise Mobility Management

Layered mobility such as mobile device managers (MDM), enterprise mobility managers (EMM), dedicated Access Point Names (APN), and encryption profiles compartment sensitive work into mission enclaves and enforces policy without advertising unusual behavior to the outside world, supporting Outer Ring discipline and Middle Ring isolation.

Secure Collaboration & Data Hygiene

Zero-trust collaboration in dedicated workspaces reduces third-party leakage during planning. Ongoing data-broker hygiene minimizes coincidental linkages that can light up an operator or family member under replay. A WIRED investigation found many brokers hiding opt-out pages from search, which explains why deletion and suppression often require persistent effort.

Training & Assessment Cadence

Progressive education and exercises – hands-on device configuration, synthetic smart-city ranges, and red-cell events with commercial data – convert doctrine into judgment under stress and feed measured outcomes back into SOPs. Where possible, incorporate PRC-style fused scenarios such as camera saturation, registry checks, and watchlist hits so teams practice staying cohort-consistent under the same pressures they will face in contested environments.

Policy & Culture

Addressing this evolving threat requires more that an adjustment to tactics. Transformational change to the mindset, culture, and policy that governs these actions is necessary to effectively meet the challenges posed by UTS.

Treat digital-signature management as mission-critical, not an IT afterthought, and tie signature metrics to readiness reporting. Assume regional diffusion of Chinese surveillance AI, which academic research shows China exports at scale, especially to autocracies and weak democracies, shaping the operating environment beyond its borders. As Lawfare argues, broader U.S. data protections would directly reduce commercial-surveillance risk and lower the mitigation burden for operators. Track three measures of effectiveness: trigger rate (how often anomalies are generated), correlation depth (how many vectors align), and reconstruction error (ambiguity after replay), and use them to drive training and resourcing decisions.

Implementation

This transition should be implemented in stages to achieve a comprehensive understanding and data-informed approach to UTS mitigation.

See Yourself: Stand up a Digital Mirror that emulates local anomaly detection (device clustering, venue cadence, cohort fit) and measures unit discoverability against city baselines. Treat this as a comprehensive UTS survey tied to commander decisions.

Shape & Control: Publish Outer Ring standards for cohort alignment, device posture, and normalized absence so occasional "no-phone" days are already part of the baseline. Pre-provision persona devices with plausible account age, app constellation, and usage cadence.

Test & Iterate: Conduct right-of-bang drills in which a red team attempts forensic reconstruction using public and commercial data. Use realistic red cells with access to commercial sensors, broker data, and building telemetry to validate DSW under smart-city conditions. Update TTPs and SOPs based on measurable ambiguity: trigger rate, correlation depth, and reconstruction error.

Consider Coalition Impact: Train, audit, and equip partners to the same Digital Signature Warfare standards. Cohesive signature doctrine reduces third-party bleed in mixed formations.

Conclusion

Visibility is normal. Obscurity is exceptional. Forces that shape their signature before, during, and after operations keep time, choice, and surprise – advantages that matter in any theater. The threat landscape is shifting faster than ever before: smart-city cameras, brokered data, and AI correlation turn everyday exhaust into targeting information, making visibility the baseline and anomalies the trigger. Digital Signature Warfare answers that reality by moving from episodic "comms discipline" to continuous, commander-led signature management across people, devices, movements, payments, and procurement. Units that institutionalize DSW through application of the Three Rings framework and measurable standards lower their trigger rate, raise forensic reconstruction error, and cut the cost of secrecy across LSCO mobilizations, sustainment flows, troop movements, and SOF missions. The objective is not to vanish, but to blend – to look like the cohort the mission demands before, during, and after the act. Forces that do this regain initiative, extend survivability, and impose uncertainty on adversary targeting and decision cycles. That is how the United States and its allies convert UTS from an asymmetric disadvantage into an operational edge, improving mission safety today and preserving strategic advantage in great-power competition.

Disclaimer: *All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or view of the US Government. Nothing in the contents should be construed as asserting or implying US Government authentication of information or endorsement of the author's views.*

Chairwoman ERNST. Very good. Thank you all very much for your opening statements.

Now we will open up for our question-answer portion of today's Subcommittee hearing, and I will yield to the Ranking Member. Ranking Member, if you would like to start with your questions, you have 5 minutes. Thank you.

Senator SLOTKIN. Thank you. Thank you, Chairwoman, and I apologize. I am going to have to step out after I ask these questions.

But super interesting topic and a topic, obviously, that deeply impacts our military, our intelligence community. I am a former Central Intelligence Agency (CIA) officer, so I am trying to imagine what the CIA officers of the future are going to be up against when

they try to go undercover abroad. Their movements, their social media profiles, their buying habits, their facial recognition is all scraped and amalgamated. But I think that this issue is one of those that overlaps with the just normal civilian population. I don't think the average person wants, you know, certainly someone from another country having all this amalgamated data.

So I guess the question I have could be for a couple of you is, Mr. Sherman, the data brokers, the people who are paying 12 cents for all the data on, you know, a military soldier or on an Army soldier's information, do you agree—I mean, I like this idea of basically changing in law that you can't just buy an American, you know, uniform military chunk of data. Does that sound right to you? Is that the way you would propose?

Mr. SHERMAN. I think that is right. The point my fellow panelists made about widening the net, I think, is really important, right? If we think about—you know, I had a data broker once say to me, oh, well, we can't sell you GPS datapoints on a military base—purely due to internal policy; there is no law that says this—but we can sell you the data on everywhere else they go and everything else they are doing all the time, right?

So, I think to that point, you know, family is one piece. If we only focus on bases, well, what about off-base activity? What about who they are meeting with? What about what they do in off hours, right, and so forth?

But I completely agree, Senator, I think cracking down on the sale in the first place is the way to go.

Senator SLOTKIN. Yes, and Mr. Stokes, I completely agree and have had legislation for years now on banning Chinese-connected vehicles from ever landing on our shores here. You described them as like a traveling cell phone. I just think it is like a traveling surveillance package.

A couple of months ago now we had an incident where some officials from Taiwan were traveling in Europe, and a car accident was precipitated right in front of the place where they were meeting. Again, I don't have the classified story on that, but my immediate thought was, how did they know where this person was? You know, what kind of vehicle was involved in collecting information or precipitating it? So I am in full support of banning those things.

But can you give us a little bit of color, you know, put on the adversary hat. If you had all this data on the U.S. military locations, individuals, et cetera, illustrate for us with a little color what kind of things you would be doing if you were the adversary?

Mr. STOKES. Thanks for the question, Senator Slotkin. That is a very charged question, but I will put it out the best way I can. Adversaries are already using this data effectively against our servicemembers and our intelligence community. We have found in our publicly available research at Ridgeline where we were tracking cohorts of data from pockets at the Pentagon, at Dulles Airport, and military installations where you look and track the commercial ad tech data at those key points. You might find, and we did find, Chinese-based cell phones with Chinese-language packs who also go to the Chinese embassies following the same cohort of individuals.

I say that to imply that it is very likely that this is a common occurrence among intelligence officers from the People's Republic of China (PRC) to disrupt or deny or even potentially cause vehicular accidents in Europe.

Senator SLOTKIN. Yes. And then last, and I am not sure who is the right person to answer this, but there is this whole competing pressure with the Pentagon where we want to protect data, and they don't have their house in order, according to, I think, all of you, but we also want to make sure that we are, you know, keeping up with the values of tech on AI and not missing out on opportunities to do interesting things. Those feel like, you know, countervailing pressures, right? And I know that there have been organizations in the past year who have been interested in data from the Department of Defense and putting that through different AI apps. What is the advice to those of us who oversee the Pentagon on how to think about AI and data and what we should and should not be doing with that data? Anybody? Don't jump all at once.

[Laughter.]

Mr. DOYLE. That is a great question, Senator. Thank you for it. It is probably also a little charged or certainly difficult to answer holistically.

I would offer, first, we face a similar challenge at Cape, which is when you want to provide people, including servicemembers, with cellular service, which everyone needs and everyone relies on. People, including national security professionals, have a very low tolerance for any compromises in that user experience, and so one of the original design principles at Cape is we have to provide uninterrupted, basically transparent user experience to our subscriber base.

I think you are describing a similar challenge, which is folks simultaneously want to be mindful of their digital footprint and careful in the way that they manage data, but they also want to leverage all these incredibly powerful technologies that are emerging literally every day all around us.

While I am not qualified to offer a specific technical solution, I would offer that what we have found over a few years of doing this now is the overarching problem statement can seem daunting and can seem intractable, but when you break it down into individual threats that you are trying to mitigate and be specific about those threats and be specific about those challenges, there is almost always a specific technical solution to be built and deployed that can uphold both your insistence on real user experience and accessibility to tools and also take care of your data privacy.

Senator SLOTKIN. Great. Thank you.

I yield back. Thank you for letting me go first.

Chairwoman ERNST. Wonderful. Thank you.

So this has been a really interesting hearing, I think, for so many of us. I know when I deployed Operation Iraqi Freedom in 2003, not many of my soldiers had cell phones. You know, all we could do was say, hey, after waiting in line for an hour to get to the one landline that we had and your 5-minute phone call with your family, just don't tell them where you are. You know, things have changed significantly from that point in time 22 years ago.

So I do see where this is an issue. I think many of you have described quite well the threats that exist out there and why that data can be so useful to our adversaries. So just understanding that what we think of as seemingly harmless information can really be leveraged not only against us, but potential units, et cetera.

Just the figure—and maybe one of you had said this—but over 85 percent of our servicemembers use connected devices that collect geolocation data, creating an exploitable surface. So our adversaries are mapping that. We need to understand that. We need to communicate that.

You have already described how these services are using the open-source datapoints to target. Mr. Sherman, you had talked about just banning the sale of that data. Is there anything else that the Department of Defense can specifically do to reduce the operational value of the information to our adversaries? And really to any one of you. Dr. Kirschbaum?

Dr. KIRSCHBAUM. Yes, so the example you gave, Senator, was really perfect because that is a classic OPSEC operation security example. When you look at the way the Department treats these things, as we have over the last 10, 15 years, they are usually the group that gets it soonest. The other security disciplines that are part of the defense security enterprise, force protection, counterintelligence, the data protection group, mission assurance, they are not as fast to come along. The good news is they are part of that security enterprise, and they are all headed by undersecretaries of defense, the right ones, the intelligence security policy, the joint chiefs, and they have a structure set out to really handle all this. It kind of warms my GAO heart. They have got roles and responsibilities. They have got a harmonization of policies. All that is the right path. What is important for them to do now is to recognize that all the things we are talking about need to be integrated into all those disciplines, and they are not now.

Chairwoman ERNST. Doesn't sound like an easy task. But yes, I do agree with you. So then how can the Department better train, then, our servicemembers to be aware and to recognize when their personal data may have been shared or, you know, exposing mission-sensitive information? What can they do? How can we train them?

Yes, Mr. Stokes.

Mr. STOKES. Thanks for the question, Senator.

UTS training or training about your digital signature is imperative for every soldier, every sailor, every airman because it is not just the person at the tip of the spear. If everybody is aware about their digital signature and what they can do about it, they then are affecting a much larger force.

At Ridgeline, we offer ubiquitous technical surveillance training and everything from 1-day chunks to several-week training. We think it is required training for the force. It used to be reserved for the special operators, and no longer is the special operator the only person that needs to care about this.

Beyond just training, I highly recommend what we call a UTS survey or a digital mirror where you have somebody collect all of that commercially available data at your unit level or your base or your squadron and look at it and tell you what you actually look

like in the data. From there, you can make more informed decisions and potentially alter your digital signature going forward.

Chairwoman ERNST. Really good.

Mr. Doyle.

Mr. DOYLE. Yes, if I may build on that. Thank you, Senator. I echo what Mr. Stokes said about the importance and value of training, although I would also point out that when we train on these UTS challenges and digital signature management challenges, often what we are trying to do is change user behavior, in particular, often but not always the way that we use our personal cell phones. In my experience and our experience, user behavior with respect to commercial cell phones is notoriously hard to alter, and there have been some high-profile examples of this.

It is not to invalidate or to minimize the importance of training or the effectiveness of training, but also I would encourage the Subcommittee to consider the importance of technical solutions and policy changes that also get at the root of the problem. I think you need a multi-pronged approach in order to be successful.

Chairwoman ERNST. Yes, thank you. Any other thoughts on that? Yes, Mr. Sherman.

Mr. SHERMAN. I would only underscore that last point, right? I agree with everything my fellow witnesses said. As we have also said, you know, national security operators are always going to have a higher burden than the average American in this area, but we can reduce it significantly with broader privacy and security controls.

So while that certainly is not, you know, only in DOD's hands, I think some of the protections we have talked about from data brokers to connected cars would do a lot.

Chairwoman ERNST. Okay. Thank you very much. I appreciate it, and I will yield back my time and will go to Senator Peters.

Senator PETERS. Thank you, Chair Ernst, for that. You know, I think this has been a great discussion. I appreciate all of you being here, and certainly, the concerns with folks in national security are very real and big, but as you know, this is a problem for all Americans. I mean, I think most Americans would be absolutely shocked if they knew what kind of digital footprint they are leaving as they just go about their daily life. And there are a lot of people, unfortunately, out there with very nefarious intent that are not targeting just our national security folks, although they are a primary target, no question about it. They are targeting everybody, criminal elements in particular. So this is something that we have to get our arms around as a country, and it is only going to get more concerning as AI continues to develop and the ability to deal with all of the data that is out there.

But before I get into data security, I would like to discuss just briefly some work that I am doing with Senator Ernst. With the creation of synthetic media, often by foreign adversaries seeking to undermine our security, the ability to verify information has become absolutely essential, I think you would all agree, for public trust, for defense, and for economic resilience. And while strong policies are necessary, which you have raised, I think it was also mentioned by Mr. Doyle, we also need technical tools. And certainly my idea as well, working with Senator Ernst, is to provide tamper-

evident transparency for photos, for video, audio, text, all those things that are out there.

In the fiscal year 2024 NDAA, I authored section 1524, requiring the DOD to pilot a digital nutrition label for media that aids in understanding the origin of digital content, for example, showing how it was made, by whom, and how it has been altered over time. In this year's NDAA, we built on that framework. Senator Ernst and I are co-leading legislation to add Digital Content Providence Act to further advance those efforts, so it is kind of all of these different approaches we are going to have to take.

But my first question is for you, Mr. Sherman, and Dr. Kirschbaum. As a ranking member of the Senate Committee on Homeland Security and Government Affairs, I recently released a report that found that Department of Government Efficiency (DOGE) is risking the sensitive data of all Americans at the Social Security Administration. According to a whistleblower, DOGE has copied Americans' sensitive Social Security data and put it into a cloud data base, according to the whistleblower, without any verified security controls in a cloud data base. This data base includes the most sensitive information, as you know, of not only all Americans, but all the military members, national security personnel, as well as their family members.

In fact, the Social Security Administration's own risk assessment warned that there is a 65 percent risk of catastrophic breach of this sensitive Social Security information. That is, of course, if that information hasn't already gone, and the whistleblowers say, we don't know. It is hard to know whether or not that is already been breached. If it has, the consequences are going to be extensive.

So, Mr. Sherman, based on your expertise, is this the kind of information in a data base that a foreign adversary like Russia and China would just love to have?

Mr. SHERMAN. Yes, thank you, Senator, and, of course, not as in the weeds of the report as what you were saying, but, yes, I will say two things, right? So one is we should always operate on the assumption that any data anywhere is of interest to adversaries, especially when it is aggregated in any kind of way. The second thing is I think there are many lessons over the last several years that we still maybe have not learned as a country from the Office of Personnel Manaagment (OPM) breach, right? Which is that, any time in particular, there is an intense—and we can give examples across administrations, but any particular concentration of the kind of data you are talking about, again, that is going to be something a foreign adversary is going to want to look at.

Senator PETERS. Yes, it is very, very important to make sure that we have the safeguards. Just to put it on an unsecured device is pretty scary. But maybe it will reassure you that the individual who oversees this data base is a 19-year-old man who was fired from his prior job for leaking data. Does that bring any comfort to any of you that this is the guy who is making sure that those foreign adversaries don't have access to that information?

Dr. Kirschbaum, could you describe the consequences if this data were given or sold to an AI company that used this information to train their models?

Dr. KIRSCHBAUM. Well, as Mr. Sherman was talking about, the lessons from the OPM breach are pretty clear. I mean, any time this data is out there and it is accessed by unauthorized personnel, it is fuel. A lot of times we are—both in the Department of Defense, based on our work, the response has been reactive rather than proactive, and these are the kind of things that we really stress with the Department because my writ is looking at the Department of Defense. We stress just leaning a little more forward, looking at what you ought to be doing versus just plugging up holes because that is never going to solve the problem.

Senator PETERS. Right. I am also deeply concerned by reports that the DOD's recent $200 million contract with Elon Musk's artificial intelligence AI company, xAI—this is the company's AI model that has a well-documented record of producing hate speech, including racist and antisemitic content. I am also concerned about the data risk for the social media company having access to DOD's most sensitive data on servicemembers as well as their families.

Mr. Sherman, what would be your top concerns about such a procurement in which a social media company could have access to DOD's sensitive data on servicemembers and their families?

Mr. SHERMAN. Yes, thank you, Senator, and I am not a content moderation expert, so I will speak to the data piece. I think this gets back to Senator Slotkin's question earlier, right, which is how do we think—I will make two points, right—at the strategic level about we want to make use of artificial intelligence or OSINT or take your pick at the same time as we are worried about security issues from it. I would say the answer is we can do both, right? Our adversaries would like to push this illusion that we can't have privacy and protection of data and successful competition, for example, right? So I would say that is the strategic point.

The policy point is I think this gets back to contracts, right? So any time any company is going through a DOD contract, especially if you are getting personnel data—and I have worked on legislation before in this area—you need to make sure there are the proper audits, security controls, other things in place, no matter what that company is, to understand what kinds of risks we are dealing with in that scenario.

Senator PETERS. Madam Chairman, can I ask one more question if I have your indulgence?

Chairwoman ERNST. Yes, go ahead.

Senator PETERS. Thank you.

Mr. Sherman, reports indicate that xAI is negotiating with foreign countries to build data centers. Such a partnership could allow the company to conduct operations in places, as you know, without core data protections and safeguards like we have here in the United States. So my question for you, what are the risks of xAI's work with a foreign country and the potential risk to the data of servicemembers and their families as they build out these data centers overseas?

Mr. SHERMAN. I would say, again, a set of criteria we can already apply, I would say, would be supply chain, right, and looking at, okay, much like we would look at who is putting the components in a connected vehicle that drives by a base. If we have a data center with data, we need to look at where is it based, what are the

law enforcement laws in that country, what are the intelligence access capabilities in that country, which other companies have controls in that supply chain to access the data? Again, these are frameworks we have, but as mentioned, maybe with past breaches and so on, we haven't necessarily learned these lessons for the military yet.

Senator PETERS. Many of those countries don't have any of those things.

Mr. SHERMAN. This is correct, yes. Many other countries do not have the kinds of democratic oversight we have over intelligence and military activities.

Senator PETERS. Particularly potential adversaries especially don't have it.

Mr. SHERMAN. China, Russia, the like, yes.

Senator PETERS. Great. Thank you.

Thank you, Madam Chair.

Chairwoman ERNST. Thank you.

Senator Kaine.

Senator KAINE. Thank you, Chair. It is a fascinating discussion. I want to ask a couple of questions that have been touched on, one about training and maybe I will start with one about the threat kind of universe.

When I came to the Senate in 2013, the discussions of adversaries' interest in our data was a little very focused on national security, data about intel officers, data about military, data about military operations. It seems like there has been an evolution during the time that I have been here that they are just interested in data on everything. Even if we don't know right now how we will use information about somebody's healthcare records or their Social Security or their consumer behavior, we just want to get it and have as clear a profile of every person as we can, and we will decide later how we are going to use it. Is that a fair, you know, kind of short form description? We have gone from real focus on national security-related data to just we want every bit of data we can get on everybody.

Mr. DOYLE. If I may, Senator Kaine, I think that is a fair observation. I think as analytic capabilities and in particular as AI capabilities have advanced and made it tractable to leverage greater and greater quantities of data, then the interest in a broader set of data makes sense. In particular, I think it is interesting to think about if an adversary were focused on creating deepfakes and creating fraudulent content, the more composite data you can compile about the subject, the more convincing of a deepfake you can make, right? At least hypothetically you can imagine if I know which pharmacy you go to, that might be useful if I were to try to create a deepfake.

I think that underscores why it is so important to identify the primary sources and the most voluminous sources of that sort of data and take a really hard look at policy changes and technological solutions to help to cutoff or otherwise make unavailable the data. Of course, telecommunications is near and dear to my heart, but there are other examples as well.

Senator KAINE. There has even been instances in recent years of foreign connected purchases of American businesses where, say, a

traditional purchase price that you might reach through like a capitalized earnings calculation, you see prices paid well in excess of that because a consumer business like a pharmacy chain or a grocery store chain not only has capitalized earnings that you can capitalize to come up with a purchase price, but they have a whole lot of data on their customer base. There is a premium that is being paid over what the actual profitability of the business is to be able to gain access to consumer data. That is starting to happen a lot.

Mr. DOYLE. Absolutely, and you can see it across industries. When businesses figure out how to efficiently monetize their subscriber data or their customer data, it becomes an entire line of business unto itself, and it is exceptionally valuable. That is true in a truly commercial sense and, of course, true in a national security sense as well.

Senator KAINE. Let me ask a question about training for our military. This is an Armed Services hearing. That question went broader than armed services. Secretary Hegseth put out some directives last week, and we are still trying to get the details, but one was I think conceptually we should try to shrink the amount of mandatory training. You don't want to have overtraining on all kinds of stuff, and he said, look, training should be really focused on warfighting.

But this is an area where it strikes me some good training for people coming into the military about how to reduce a digital footprint that can be weaponized against you or weaponized against the American military would be a good thing. So I would like to hear about training, although, Mr. Doyle, you were a little bit skeptical and you said, you know, people's propensity to use their devices is such that training hasn't necessarily proven to be that effective in getting them to make the change. But, you know, for somebody entering into the military where they are going to have access to a lot of information that we would want to keep more, you know, close to the vest, what would your thoughts be for Armed Services Committee members about the kind of training we should be offering on this ubiquitous surveillance problem?

Mr. STOKES. Senator Kaine, thanks for the question. I will just throw out before Mr. Doyle that we recommend a comprehensive and cohesive strategy for UTS-based training. I think if you did this early within a servicemember's time within the Department, they would have the tools and capabilities to grow that as needed. Secretary Hegseth is right. You don't need to have weeks upon weeks of UTS-based training.

Senator KAINE. Yes.

Mr. STOKES. But I do think having a modicum of training at the beginning of their career and periodic throughout their career would be——

Senator KAINE. Maybe different levels of training——

Mr. STOKES. Hundred percent.

Senator KAINE.—depending on what your MOS would be. So everybody could get a base level right at the beginning, but then as you progress, depending upon what your position is, you might need——

Mr. STOKES. Absolutely.

Senator KAINE. Yes. Other thoughts on the training issue?

Dr. KIRSCHBAUM. Yes, we have outstanding recommendations of the Department on this issue. As Senator Slotkin alluded to, warfare has changed. The information environment is very much like a domain amongst everything else. So we have had recommendations of the Department to look at how they train commanders and on down on how to deal with the information environment. It goes down to the unit level to some degree as well. And they have made some progress in seeing the value of those, but as I said, it is kind of diffuse.

We have examples of Air Force and Army units kind of assessing where they are in their own digital profile, but that needs to be expanded out writ large to the Department and beyond, apropos of your first question. But that is a lot of effort and a lot of prioritization and money to do that.

Senator KAINE. Can I continue a little bit, Senator Ernst?

Chairwoman ERNST. Certainly.

Senator KAINE. Dr. Hirschbaum, you said something, I think it was in response to a question maybe from Senator Slotkin where you had this paragraph that said the GAO really likes that they have done all these things right, but there is something that they are not yet doing right. Can you go back and say that to me again so I can understand it?

Dr. KIRSCHBAUM. So if you read GAO reports, you will find a pattern. When we are looking for progress on something, whether it is implementation of a strategy, we are looking for several things. Who is supposed to do it? How do they know they are going to do it? What timelines are they working on? And how will they know they have achieved the ends they were trying to set out for? And those are all set out—in case you are having trouble sleeping at night, I can send you reports that will outline all this for you. Those are the kind of things we would like to see. Those are things that are guarantors of progress in some way, shape, or form.

Then, obviously, leadership. They have that structure in the defense security enterprise. If you look, it is people from the entire OSD, the Joint Staff services, they are all responsible in different ways. There are all these security disciplines. They have got that structure set out. It is a matter of applying the existing structure to this newer problem set.

As I said before, like the operations security people, they are more onboard, some of the other disciplines, not as much. Once they are more acclimated to caring about this, that existing structure will serve them well.

Senator KAINE. Okay, thank you, and then one last thing, if I could, just really more of a comment.

I am on the HELP Committee too—Health, Education, Labor, Pension—and I am sort of thinking about this discussion in light of, you know, what do we teach young people about digital footprint? On the HELP Committee, we also deal with abuses of elders on all kinds of scams that people fall victim to. Obviously, having more information about individuals makes your scamming much more likely to be successful because you can be really targeted in terms of going at somebody's known vulnerability.

So this is a hearing that has got my wheels turning not just on the Armed Services Committee but in thinking particularly on this

training issue, you know, kind of thinking about the ways we need—we tell children don't accept candy from strangers or, you know, don't talk to somebody you don't know. I mean, we are trying to protect children's privacy. We always have. This is a new threat that I am not sure we are, you know—well, I know we are not as thoughtful yet as we should be about trying to equip people with an appropriate wariness about—I mean, a lot of good comes from this, but we are not doing a good job of necessarily teaching people to be skeptics, and I think we need to do more. So thank you for holding this hearing, Senator Ernst.

Chairwoman ERNST. Absolutely, and I do appreciate the conversation today. Rand had done a study not all that long ago of DOD personnel and found that only about 72 percent of those surveyed had actually had training about data brokerages, about their digital footprint. You are right, Senator Kaine, that there are so many other applications here not just in the DOD space but everywhere else across the United States.

I am curious. I am sure that many other countries have this same discussion. Are any of you aware of what maybe other allies or adversaries are doing in this space as well to protect their own citizens?

Mr. SHERMAN. I will offer two as an example. So one is I referenced the Department of Justice stood up a bulk data broker national security program, does not deal with certainly all of the issues we are talking about here but attempts to take a chunk out of it. The United Kingdom is now mimicking that program, essentially saying, okay, also we have lots of things going on in this area. This is one way we want to kind of take a swing at the problem.

The second is—and I preface this, we of course—this does not mean we should be replicating everything China is doing, but the Chinese Government in the last several years, for example, has greatly restricted the outbound transfer of genetic data on Chinese citizens, greatly restricted all kinds of ad tech and other things going on there. So if we think about it at the macro level, there are steps that some adversaries are taking. Russia has made dramatically less open-source information available to the West since the war. So there are ways our adversaries are trying to, you know, successfully or not at least knock this down a little bit. I think, again, that stands in contrast to really important work at the operational level but less at the strategic level in the U.S.

Chairwoman ERNST. Yes, Mr. Doyle.

Mr. DOYLE. Thank you, Senator Ernst. I would build on that maybe in the more operational context and more in the national security context to say that in my observation, our allies take their cues heavily from the United States' leadership on this front, and so what I think that means for this committee is that investments or progress we can make on the technology front or on the policy front have, you know, obviously impact right here but also impact among our close allies.

Chairwoman ERNST. Wonderful. Thank you.

Yes. Yes, go ahead, Senator Kaine.

Senator KAINE. I am giving a talk with Senator Sheehy, and I need to walk out, but I am going to ask a question for the record

and just to alert you to it. Is there anything in the regulation of data centers in the United States that could be done that could be sort of an upstream way of helping us deal with that challenge? There are all kinds of data center issues about, you know, the power demand and other things that are going on, and we wouldn't want to do regulation that would make data centers—you know, people would—we wouldn't want folks to say, well, we are not going to build in the United States, we are going to build elsewhere because we don't want to have a regulatory regime that is too constricting.

I will ask that question for the record, but just to alert you that it is coming. I would be curious to your thoughts on that.

Chairwoman ERNST. Yes, absolutely. Thank you.

We will go ahead and conclude today's hearing on the Emerging Threats and Capabilities Subcommittee and really appreciate the time and attention you have given to this.

Many of us are heavily invested. Senator Peters mentioned a bill that we are working on together, and it focuses a lot on the AI space and making sure that any digital images or products are authenticated. So we will continue working on that, but you have given us a lot of food for thought in many other areas.

So, again, thanks to our witnesses for taking the time today. We appreciate it.

With that, we will go ahead and close the hearing.

[Whereupon, at 3:27 p.m., the hearing was adjourned.]

○