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/b1f697ce-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.