Stenographic Transcript
Before the

Subcommittee on Emerging Threats and Capabilities

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

TO RECEIVE TESTIMONY 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

Tuesday, October 7, 2025

Washington, D.C.

ALDERSON COURT REPORTING
1029 VERMONT AVE, NW
10TH FLOOR
WASHINGTON, DC 20005
(202) 289-2260
www.aldersonreporting.com

TO RECEIVE TESTIMONY 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

Tuesday, October 7, 2025

U.S. Senate
Committee on Armed Services
Subcommittee on Emerging Threats and Capabilities
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:28 p.m., in Room SR-222, Dirksen Senate Office Building, Hon. Joni Ernst, chairwoman of the subcommittee, presiding.

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

OPENING STATEMENT OF HON. JONI ERNST, U.S. SENATOR FROM IOWA

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.

And 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 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 service members 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.

[The prepared statement of Chairwoman Ernst follows:]

Chairwoman Ernst: And with that, then I will turn to the ranking member.

STATEMENT OF HON. ELISSA SLOTKIN, U.S. SENATOR FROM MICHIGAN

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. And 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 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.

And back over to you, Madam Chairwoman.

[The prepared statement of Senator Slotkin follows:]

Chairwoman Ernst: Wonderful. Thank you. And 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 five 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, 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 CEO of Global Cyber Strategies, a Washington, D.C.-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.

And 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.

And with that, we will start with you, Dr. Kirschbaum, and you are recognized for five minutes.

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

Mr. 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 service members, 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.

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 service member and/or family members through the aggregation of information and sources. A service member'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 service members or relative social media sites and associated information and data tags. And 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:]

Chairwoman Ernst: Thank you, Dr. Kirschbaum.

And Mr. Sherman, you are now recognized for five 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 two 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 service members 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 U.S. 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 U.S. 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 service members with virtually no serious background checks or vetting for as low as 12 cents a service member 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 U.S. military forces. Moscow, likewise, has advanced cyber and intelligence functions and many 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.

And 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 service members 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:]

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 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 service members 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 service member, 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 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, buying 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 '26 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 service member 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.

[The prepared statement of Mr. Doyle follows:]

Chairwoman Ernst: Thank you, Mr. Doyle.

Mr. Stokes, you are recognized for five 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 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 service members 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. Stokes follows:]

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

And now we will open up for our question-answer portion of today's subcommittee hearing. And I will yield to the ranking member. And, Ranking Member, if you would like to start with your questions, you have five 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 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. And 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. And 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?

And 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: Yeah. 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.

And 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 service members 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. And 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 PRC to disrupt or deny or even potentially cause vehicular accidents in Europe.

Senator Slotkin: Yeah. And then lastly, 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

service members, 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.

And 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.

And 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 five-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 service members 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.

So 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?

Mr. Kirschbaum: Yeah, so the example you gave, Senator, was really perfect because that is a classic OPSEC operation security example. And 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 service members 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 one-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 '24 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 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 database, according to the whistleblower, without any verified security controls in a cloud database. This database 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. And 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. And 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 database that a foreign adversary like Russia and China would just love to have?

Mr. Sherman: Yeah, thank you, Senator. And, of course, not as in the weeds of the report as what you were saying, but, yeah, 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. And 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 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: Yeah, 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 database 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?

Mr. 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. And 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 service members 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 service members and their families?

Mr. Sherman: Yeah, 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. And I would say the answer is we can do both, right? And 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 service members 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? And, 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: And 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: And 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. And 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 cut off 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. And so 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 service member'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: Yeah.

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: And 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: Yeah. Other thoughts on the training

issue?

Mr. Kirschbaum: Yeah, 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.

And 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?

Mr. 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.

And 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.

And 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? And on the HELP Committee, we also deal with abuses of elders on all kinds of scams that people fall victim to. And, 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. And 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. And 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.

And 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. And 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: Yeah, absolutely. Thank you.

And 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.

And 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. And 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.

And with that, we will go ahead and close the hearing.

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