The Army Cyber Institute
United States Military Academy, West Point, NY

Death by a Thousand Cuts: Commercial Data Risks to the Army

Executive Summary

This report outlines the force protection challenges related to publicly available information (PAI), and specifically highlights commercial data exposed through data brokers. The rapid, widespread, and low-cost availability of data about personnel poses significant operations security (OPSEC) and force protection vulnerabilities for the Army. The recommendations for action included in this report emphasize organizational mitigation actions, as opposed to individual training or national-level policy changes. These are actions that the Army can implement with existing authorities – in absence of federal data privacy legislation or DoD directive – to protect the force while preserving the civil liberties and privacy of its members. While many of the analytic technologies outlined in this report are touted as the Industry standard for marketing, they are widely viewed as invasive by privacy and civil liberties experts - while granting users little transparency or control over what data is collected about them.

Key Points:

- Data on Army servicemembers, personnel, and family members is available at a low cost per person/record and easily available for purchase online.
- There is currently no national data privacy legislation that protects Soldiers (or any U.S. citizens) from the vulnerabilities created by data brokers.
- The accuracy and quality of the data available for purchase from commercial data brokers has not been confirmed by the Army or the DoD.
- In addition to explicit affiliation data, multiple benign data types can be combined to reveal military affiliation and other operationally relevant information.
- The data made available by commercial brokers includes traditionally sensitive data types including demographics, PII, and medical information.
- This commercial data creates a range of vulnerabilities that facilitate recognized foreign intelligence threats and physical harm without the need for the resources of a nation-state.
- The Army has options available to address PAI problems and should not over-rely on encouraging (via annual training) individuals to take action on their own.

Highlighted Recommendations:

This report recommends that the Army adopt frameworks for assessing risk resulting from PAI, along with other essential policy, technical, resourcing, and contracting recommendations to address commercial data vulnerabilities. A complete list of recommendations is presented in Section 6.

- Provide a data broker opt-out service to all servicemembers, civilians, and families by creating an internal capability or by purchasing a commercially available service. [Technical/Resourcing]

- Restrict third-party commercial data collection, telemetry, and trackers on DODIN-A networks and Army-furnished devices (e.g., computers, smartphones). [Technical]

- Expand the use of Login.gov or DS Login to other government entities to minimize the use of commercial identity management companies like ID.me. [Technical]

- Army senior leaders can communicate the risks and observed impacts of publicly and commercially available data to inform state and federal legislation regulating the collection, packaging, and sale of personal information. [Policy]

- Integrate and refine commercial PAI risk management as described in ADP 3-13, into existing organizational policies and doctrine - to include ADP 3-37 (Protection), ATP 3-13.3 (OPSEC), and others. [Doctrine]

- Create a dedicated, NSA-certified Army Red Team to assess friendly signatures created by Army personnel and operations available in PAI, similar to what is currently done in the OPSEC and cybersecurity fields. [Resourcing]

- Develop a Home Use Program for privacy-enhancing technologies. [Resourcing]

Authors:

Jaclyn Fox

Alexander Master

Nicolas Starck

Jessica Dawson

1. Introduction

This report outlines the broad force protection challenges faced by the Army related to publicly available information (PAI) and its potential for exploitation by malign actors. Section 2 of this report provides background context for the problem space. Section 3 presents a proposal for a Data Risk Framework, nested in the Army Risk Management Framework, to assist decision-makers in understanding what data may create vulnerabilities for their personnel, unit, or operations. Sections 4 and 5 highlight prior research that informed the Data Risk Framework, and expand on the 2023 data broker report by Duke University - funded by the Army Cyber Institute - that demonstrated data broker industry practices related to servicemember data. Section 6 proposes actions that the Army can take using existing authorities to protect service members from commercial data collection while preserving the civil liberties and privacy of the force. Finally, section 7 proposes future research efforts.

The principles of offense and defense are the foundations of Army doctrine, where the defense sets conditions for the offense. Historically the United States has been fortunate to have two oceans between it and its foreign adversaries, providing for a robust defense anchored in geography. However, technology and the data collection it has enabled have transformed competition and conflict between nations, eroding this historical advantage and challenging the Army's ability to secure essential elements of friendly information (FFI) from malign actors. Commercial data collection[1] outside of the Army's control enables continuous surveillance of the force and their families. To succeed in this modern operational environment, the Army must assess and mitigate the risks to the force from what the U.S. government has defined as Ubiquitous Technical Surveillance (UTS), or what is generally known as the "surveillance economy."[2] This report uses UTS to describe data collection and aggregation efforts that occur in the course of conducting daily life in modern society. Publicly Available Information (PAI) is the aggregated data that often arises from this collection.

PAI, collected from various sources including medical records (despite HIPPA protections), government records, home addresses, personal phone numbers, social media accounts, online purchase records, credit reports, and mobile device location data[3] is aggregated and sold by commercial brokers – making it available for use by anyone who can afford it.[4] This data may be grouped into discrete "audience segments"

---

[1] Christl, W. 2017. Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. http://crackedlabs.org/en/corporate-surveillance
[2] Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism. PublicAffairs Publishing.
[3] Sherman et al., 2023. Data Brokers and the Sale of Data on U.S. Military Personnel. Page 44. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel
[4] Poulson, J. 2021. Easy as PAI. Tech Inquiry. https://techinquiry.org/EasyAsPAI/

to provide tailored sets of information about particular groups of individuals. The data brokerage economy is global and has very little regulatory oversight or control.[5]

The scale and extent of PAI collected represents an important force protection issue that the Army, as an organization, should take seriously. The same concerns that the U.S. Government has about data collected by TikTok resides in commercial data brokers – the difference is far less visibility about who the key entities are in this ecosystem.

A recent study funded by the Army Cyber Institute and conducted by researchers at Duke University demonstrated that U.S. servicemembers and their families are one such tailored audience segment.[6] The Duke report chronicles the procedures through which these data can be legally obtained at low cost, by domestic or foreign entities. The report also highlights the inconsistent controls, identity validation requirements (in several cases, none), and rules enforced by each broker. Duke's researchers focused on a sample of 12 data brokers and executed purchases from three brokers, representative of a relatively small sample of the estimated 5,000 global data brokers.[7] This report will not rehash the wide range of academic and public reporting about commercial data collection but rather extends the findings and recommendations to the broader force protection implications of it.

2. Background

Ubiquitous technical surveillance (UTS) and PAI are force protection and operational security (OPSEC) issues. Current doctrinal conceptions of friendly data and information tend to focus on data created and controlled by the Army. However, as the new Army Information doctrine acknowledges, data and information outside of the military's control can have operational consequences.[8] Furthermore, the Army often has limited authorities to sense and mitigate this commercial collection. Sensing and articulating the risks associated with public and commercial data are necessary to create effective mitigation strategies.

As society progresses, technology is ever-increasingly present in daily life. Modern technology is driven by data. UTS describes the "widespread collection of data through visual, imagery, electronic communications, financial transactions, domestic and

---

[5] Sherman, J. 2021. Data Brokers and Sensitive Data on U.S. Individuals Report. https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/
[6] Sherman et al., 2023. Data Brokers and the Sale of Data on U.S. Military Personnel. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel
[7] Twetman, H. and Bergmanis-Korats, G. 2020. Data Brokers and Security – Risks and vulnerabilities related to commercially available data. NATO Strategic Communications. https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf
[8] ADP 3-13: Information, November 2023

overseas travel, and online presence."[9] The ability to collect, aggregate, and correlate individual data points and process them at scale has primarily been driven by commercial incentives to market products to individual consumers. These advances can lead to convenience for consumers and record profits for businesses. Unfortunately, this same information that is used for marketing can be used to target an individual in their home, commit identity fraud, harassment, or target groups as part of an influence campaign.

The risks these data vulnerabilities pose are not hypothetical. A 2022 GAO study showed how PAI derived from ubiquitous technical surveillance can foreshadow or reveal a military deployment[10] as well as reveal information about key leaders. Online advertising conducted via companies such as (but not limited to) Alphabet (aka Google) and Meta (aka Facebook, Instagram) can be a significant source of exposure. A recent report from the Irish Council for Civil Liberties (ICCL) highlighted how real-time bidding for ads enables attackers to develop in-depth profiles on military and senior government officials.[11] The Duke report, however, is one of the first publicly available investigations to demonstrate that military personnel data is available for sale to domestic and foreign buyers at low cost.

Sensors in the commercial surveillance ecosystem collect *on everyone*. While much of the reporting on commercial data collection focuses on social media's data collection practices, this is far from the only source of data. There is relatively little known about the true origins of the underlying data provided by any given broker, as it comes from a variety of sources and devices. For example, many states allow the Department/Bureau of Motor Vehicles to sell data.[12] Cell phones and computers are widely recognized as common sources of personal consumer data. However, vehicle telemetry is also a source of data that it is impractical to "opt-out" of collection. It is nearly impossible to buy a new car that does not come with tracking and surveillance data collection - which is justified and frequently marketed as improving consumer safety or

---

[9] FY23 Operations Security Presentation. 2022. Naval Information Forces. https://www.navifor.usff.navy.mil/Portals/48/OPSEC/May%202023%20uploads/FY23%20OPSEC%20GMT.PPTX

[10] GAO. 2022. GAO-22-104714 Information Environment: Opportunities and Threats to DOD's National Security Mission. https://www.gao.gov/assets/730/722922.pdf

[11] Ryan, J. and Christl, W. 2023. America's Hidden Security Crisis: How Data About United States Defense Personnel and Political Leaders Flows to Foreign States and Non State Actors. Irish Council for Civil Liberties (ICCL). https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf

[12] Sterman, J. and Brauer, A. February 2020. Depending on where you live, your DMV may be selling your personal information. WJLA. https://wjla.com/news/spotlight-on-america/depending-on-where-you-live-your-dmv-may-be-selling-your-personal-information

experience.[13] As a result, the ability for individuals to know, let alone control, what data is collected about them is limited.

Even if it were possible to solve the "opt-out" dilemma, this is not an individual-level problem – the Army should recognize that this data is widely available and creates force protection vulnerabilities, regardless of whether individuals recognize the risk or not. Publicly available data provides a vast trove of information that is also available to adversaries and malign actors.[14]

Limitations in Existing Law

Current legal frameworks in the U.S. provide few avenues to limit or restrict data collection."[15] National privacy legislation - such as the Fair Credit Reporting Act, the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act (FERPA), and the Children's Online Privacy Act (COPPA) – do not address the overarching problem of data brokers or Ubiquitous Technical Surveillance (UTS). Many of these laws are sector-specific, only apply to particular entities (e.g., federal government agencies, healthcare providers, financial institutions), or were written before the proliferation of Internet-based communications. No federal comprehensive data protection law currently exists. Several U.S. states have passed consumer data privacy legislation[16] (e.g., California, Colorado, Connecticut, Virginia, Utah) which provides Soldiers and family members with residence in those states with some rights to "opt-out" of their data being sold or the right to request that their personal information be deleted. This leaves significant gaps in coverage for some Army populations (e.g., Fort Liberty, North Carolina; JBLM, Washington). Even in states with privacy legislation, these laws are reactive – allowing for deletion or correction of data that has already been collected – as opposed to requiring an "opt-in" consent to data collection in the first place.

3. Framework for Assessing Data Risk

While the Army has doctrine for assessing information risks, these frameworks were tailored toward data created and controlled by the Army. The Army must adapt its

---

[13] Caltrider, J., Rykov, M., and MacDonald, Z. September 2023. Privacy Not Included: A Buyer's Guide for Connected Products. Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[14] 116th Congress. (2017). REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION (Senate Report 116–XX). United States Senate Intelligence Committee. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

[15] Waldman, A. 2023. Advanced Introduction to U.S. Data Privacy Law. Edward Elgar Publishing.

[16] International Association of Privacy Professionals (IAPP). https://iapp.org/resources/article/us-state-privacy-legislation-tracker

doctrine to assess and mitigate the risks created by UTS and PAI. The proposed data risk framework is intended to bridge this gap and serve as a guide for Army leaders to assess the risks that may be present from commercial data. We demonstrate the vulnerabilities in the data broker ecosystem highlighted by the Duke report by providing a deeper dive into one of the larger data brokers and the variables that are available for purchase.

The Data Risk Framework

The ACI has developed a data risk framework to help guide the assessment of the risks nested within the existing Army risk management doctrine. This framework provides a heuristic mechanism to conceptualize what kinds of data are commercially available as well as what types of threats have access to them and importantly, what vulnerabilities are available for legitimate purposes but also for exploitation.

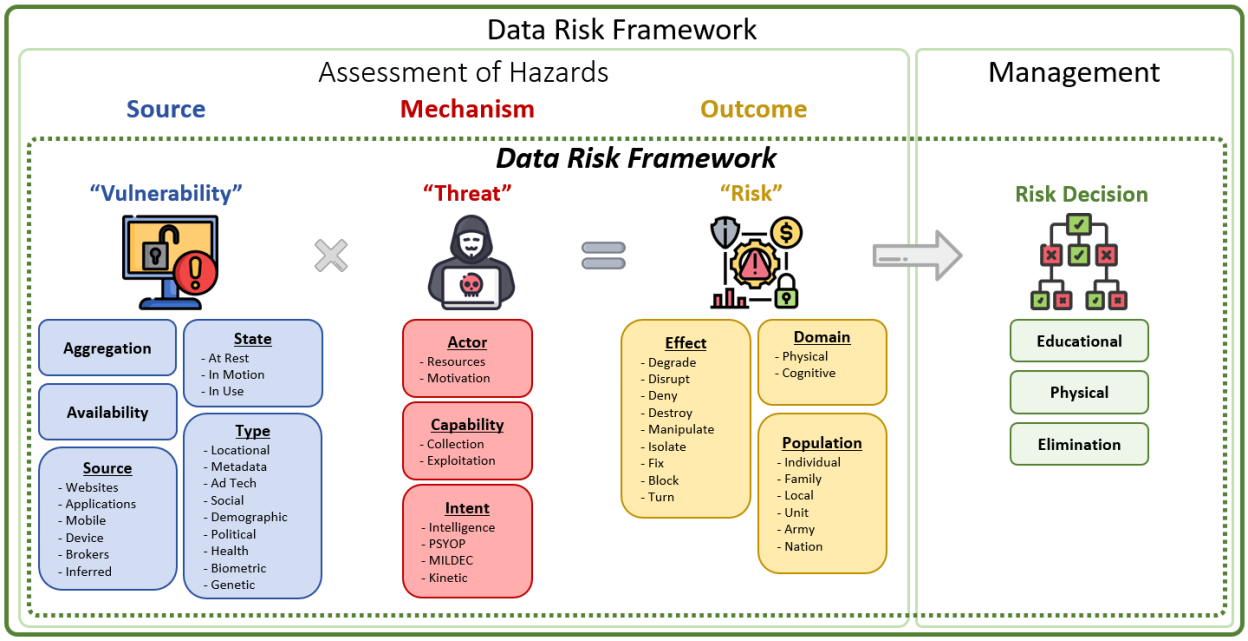

Figure 1: The Data Risk Framework

The proposed Data Risk Framework is meant to help decision-makers and their staff anticipate the risks associated with data that may be available to malign actors. This framework is intended to connect PAI concepts to their existing risk to make informed risk management decisions. By engaging the staff in conceptualizing the potential connections between available data types to organization-specific interests and risk outcomes, this framework can guide prioritized mitigation actions. While the framework accounts for available data types and threat actors, it abstracts these factors to enable a

broader force protection process than currently exists without requiring access to specific PAI (preserving fundamental civil liberties and privacy) or specific threat intelligence.

4. Prior Work Assessing Data Risk

Vulnerabilities created by Data Brokers

While the framework above illustrates the variety of publicly available data, this section goes deeper into the risks exposed by data available for purchase from at least one large data broker. While the researchers in the Duke study purchased data explicitly related to military servicemembers and their families and provided a sample of variables they were able to purchase, researchers at the ACI examined commercially available audience segments available in a dataset published by the Markup and attributed to the data broker Xander, which is Microsoft's ad platform.[17] Understanding the scope of commercial data available on military personnel and their families is essential as military data may be cross-referenced with other variables not specifically acquired on military populations and/or sensitive variables may be geo-located to military spaces. Given the growing capabilities of artificial intelligence, even if this data is not a vulnerability today, that does not mean it won't feed emerging vulnerabilities in the coming years. In this report, which expands on the Duke report, we are specifically interested in the potential of this data to be weaponized against national security through the *identification and cultivation of force protection concerns in commercial data available for sale/transfer through data brokers*. Future reports will expand on other vulnerabilities in the commercial surveillance economy.

[17] Keegan, J. and Eastwood, J. June 2023. From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You. The Markup. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you

Dataset #1 (Broker 3)	Dataset #2 (Broker 3)	Dataset #3 (Broker 3)	Dataset #4 (Broker 4)	Dataset #5 (Broker 6)
Contact data on 5,000 active-duty personnel $0.20/servicemember Name, home address, email, specific branch and/or agency – such as "Marine Corp", "Coast Guard", or "Federal Employment – National Security"	Contact data on 5,000 friends and family members of active-duty personnel $0.20/person Name, home address, email, specific branch and/or agency affiliation	Ailment and health condition data on 15,000 active-duty personnel $0.22/servicemember Name, home address, email, "Individual ID", and data (checkbox) on 15 different ailments or conditions including: Alzheimer's disease, heart conditions, asthma, bladder control difficulties, diabetes, hearing difficulties, high blood pressure, migraines, physical disabilities	Contact data on 5,000 active-duty personnel $0.125/servicemember Name, home address, email, cellular phone number	Contact, demographic, political, and financial data on each active-duty servicemember in its records (4.95 million records) geofenced to D.C./Maryland/Virginia area $0.213/servicemember (initially $0.245) Name, home address, email, political affiliation, gender, age, income, net worth, credit rating, occupation, presence of children in the home (Y/N), marital status, homeowner/renter status, home value, and religion

Figure 2. Variables purchased from various data brokers in the Duke data broker report (Sherman et al. 2023)

While our analysis did uncover additional specific data points related to the U.S. military, including sensitive information regarding the use of military-affiliated banking institutions, the bulk of our report will focus on the audience segments collected for the general population that can be used to directly undermine U.S. national security when cross-referenced with data on U.S. servicemembers, their families, and other individuals holding government positions with access to classified information.

The Xander Dataset

Using a database of 650,000 audience segments across 93 sellers, researchers at the Army Cyber Institute add more depth to the recently published Duke Data Broker study to understand the full scope of data availability. In the Xander dataset, published online, we identified military-identified audience segments. This is because, through cross-referencing of military identification or geo-fencing of variables in military locales, one should be able to get any of the specific, intimate, data points in the broker catalog even if not explicitly identified as military data.

From the commercially available data, anyone with the means can cheaply and easily acquire lists of individuals, such as:

- *Gun owners with handgun conceal carry permits who are recently divorced and drinking excessively*
- *"Affluent Jews" who are registered as Democrats in a particular geographic area*
- *Conservative Christians who are registered as Republicans in a particular geographic area*

- *Individuals who have recently been geo-located to a pregnancy clinic or have purchased Plan B over the counter*
- *Those who self-describe as "patriots" and voted against the current administration*
- *Individuals with large debts, bankruptcy, or in need of immediate loans*

The authors selected the above data points because of their sensitive nature and highlight that anyone who wishes to could purchase these segments. At very low cost, a malign actor can gain access to the contours of individuals' lives *at scale*, highlighting pressure points that could be used for targeting, blackmail, or other forms of exploitation.

Military Friendly Banks

Many financial institutions within the banking industry, despite being regulated, leverage tracking technology on their websites. Installation of tracking pixels on commercial websites is a standard and widely used business practice today. However, few companies seem to be cognizant of the amount of data that they are sending to data brokers and other ad tech companies, nor do they seem to be aware of how this data can be used against their customers. Banks that cater to military populations are no different. However, the risks associated with their membership present greater force protection concerns.

For military personnel, commercial data collection can reveal information about recent or upcoming deployments, mental health vulnerabilities, divorce or infidelity, abuse situations, or even routine medical care such as pregnancy or miscarriages. Providing data to data brokers is not a value-neutral decision – it is assuming risk on behalf of their customers, which has larger implications not only for their customers but for national security.

Another article from The Markup demonstrates how this data collection can be instrumented in practice, packaging descriptive information about individuals into discrete "audience segments" available for purchase. For example, information from the USAA trackers is re-packaged to target individuals who have accounts with USAA.

Branded Data > AdAdvisor by Neustar > Personal Finance > Financial Institutions > Has Financial Accounts With USAA (BlueKai)

Segments also include prospective account holders, those likely to hold accounts, likely to make purchases with a USAA credit card and likely to respond to emails from USAA. With this information, individuals could easily be targeted by malicious actors stating that there is something wrong with their USAA account and demanding personal

identifying information in order to correct it. The fact that malicious actors would know not only that individuals had affiliated accounts but the type of account could lend legitimacy to their scam and increase vulnerability for military members and their families. Segments get even more fine-grained, however, and include individuals who use banks' mobile apps, are "heavy" usaa.com website visitors, and visit branches in person. Again, this increased granularity may lend credence to scams and increase the likelihood of military members and their families being misled. Of note, USAA is not the only military-affiliated financial institution captured in the commercial data; banks like the Navy Federal Credit Union, Pentagon Federal Credit, and others also leave their customer base exposed.

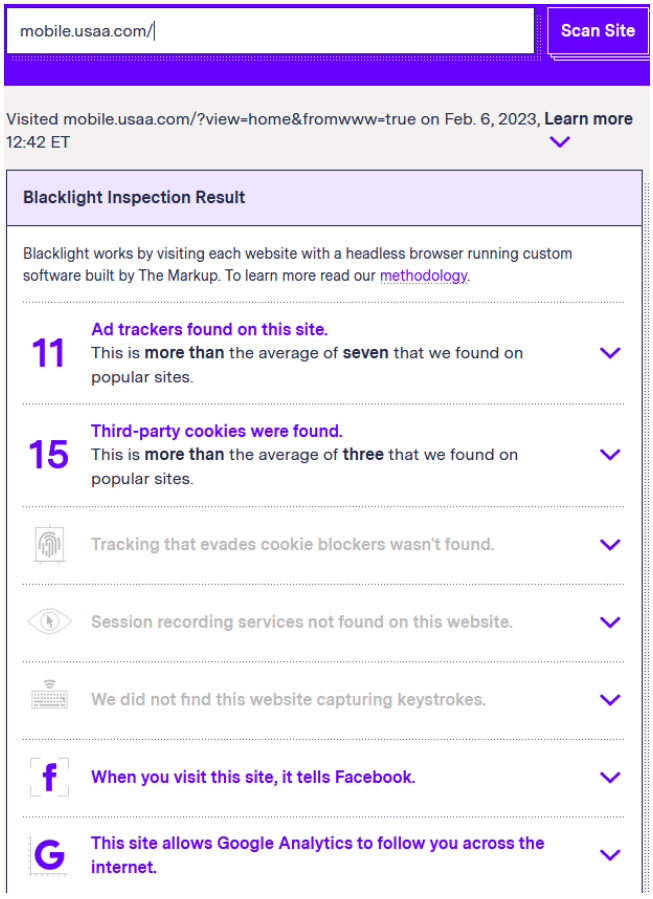

Figure 3. Blacklight Assessment of usaa.com

In addition to common third-party tracking cookies or pixels (e.g., Google analytics and Meta pixel), some of the military-friendly banks also include trackers from a company called Neustar, which, according to their website, is now part of Transunion TruAudience™ that promises to help advertisers "transform omnichannel media

performance with… identity-driven marketing capabilities."[18] Transunion is one of the major credit reporting agencies whose credit scores regularly shape financial outcomes for individuals and, along with other credit reporting companies like Experian, is now selling identified data about its customers to marketers. This includes data about likely military service members and information gathered from military-friendly banks can help complete the data picture. This data collection can be instrumentalized in practice, packaging descriptive information about individuals into discrete "audience segments" available for purchase.

Military Discounts

Foreign adversaries have demonstrated their willingness to target domestic populations using military personnel as well as veterans. Veterans have been targeted for scams on holidays like Veterans Day, which target them on a day more known for sales than tributes to veteran service, and by churches seeking to defraud veterans of their GI Bill benefits.[19] Military discounts are one of the more insidious ways to collect information about veterans online. Verizon Fios customers cannot receive a military discount without verifying their identity through ID.me - an identity management broker that veterans can opt into to receive online military discounts - rather than showing a military identification card at the register. Other companies such as Dell, HP, and Apple, travel companies like Hotels.com and Jewel Resorts among others, and casinos like Caesars Palace encourage people to verify their military status through online registration using ID.me. Online businesses will often only honor a military/veteran discount if the consumer uses ID.me; they provide no other means to validate their service connection. This information can subsequently be used to target veterans for fraud or influence purposes. A vendor that uses a service such as ID.me inherently gains access to a validated list of individuals with military affiliation.

[18] TruAudience. (n.d.). Retrieved December 12, 2023, from https://www.transunion.com/solution/truaudience

[19] Hughes, S. January 2023. Exclusive: Church Preyed on Veterans and Stole Millions, says DOJ. Court Watch. https://www.courtwatch.news/p/exclusive-church-preyed-on-veterans

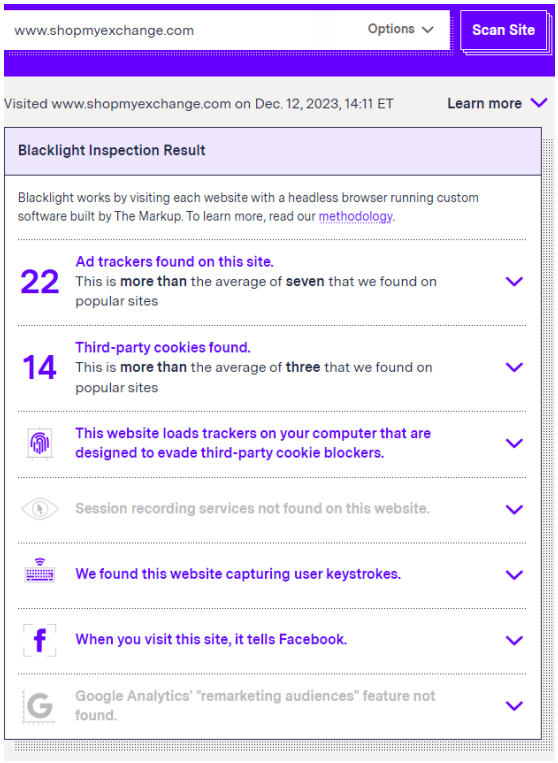

Figure 4. Blacklight assessment of the shopmyexchange.com website

AAFES, the Army Air Force Exchange Services, contains an above average number of trackers on its sales website. The main aafes.com website only had one analytic tracker present, but the shopmyexchange.com website had significantly more than industry standard tracking technology. Blacklight detected 22 ad trackers, 14 third-party cookies, keystroke logging software, and browser fingerprinting capabilities. When AAFES leadership was informed of the issues related to trackers on their website, they responded that they were launching a new site that would address most of these concerns and that AAFES's General Counsel office would review all privacy and data policies. They addressed the unusual number of trackers as a result of them switching between two different analytics providers. Further, their Information Technology team added an additional assessment process requirement specific to third-party code and components on public-facing websites operated by AAFES.

Commercial Data Force Protection Vulnerabilities

Malign actors can target individuals based on psychosocial predispositions and life stressors that make them vulnerable to engaging in insider threat behaviors. These include:

- Psychological traits: personality traits, thrill-seeking behaviors, narcissism, reactivity to stress
- Behavioral/Physical health concerns traits: substance abuse, use of testosterone, mental health
- Recent life stressors: death of close family members, divorce, domestic abuse

Third parties can further target this group by potential motivations for engaging in actions against their organization. Variables are present in the dataset that represent key motivations for engaging in insider threat behavior: money, influence, power, ideology, and workplace resentment.

- Finances: debt, loans, bankruptcy, recent dramatic changes in finances
- Ideology: moral qualm with organization (represented through various audience segments about specific ideological positions that may or may not be represented by the organization an individual works for)
- Workplace resentment: feeling overqualified or disengaged at work; low job satisfaction

Audience segments are available that delineate individuals by cohesion corrosives including race, religion, ethnicity, and sexuality. This allows an external actor to engage in targeted information operations making salient force divisions and fomenting violence and disunion. Audience segments are also available which allow malign actors to target U.S. servicemembers with children who have special needs, mental health, or other vulnerabilities.

In sum, PAI from commercial sources can be used to target force readiness through cohesion corrosives, blackmail, and other vulnerabilities (e.g., targeting an individual's children). This report demonstrates how easily available "audience segments" built for targeted advertising highlight the depth of information being collected on not only average citizens but also military personnel and their families. This data has significant ramifications not only for individual privacy but also as a potentially serious force protection issue. The Army should not wait for a smoking gun to take action to minimize the risks to the force.

5. Other Mitigation Frameworks

Please see the enclosures included in the Controlled Unclassified Information (CUI) version of this report for other frameworks, created by the Central Intelligence Agency, that the Army could use to assess the risks of how PAI and CAI may be used against service members for malign influence. The CUI report and enclosures are available at https://www.milsuite.mil/book/groups/army-cyber-institute/.

6. Recommendations

The Army should prioritize organizational mitigation actions that can be implemented on behalf of Soldiers to supplement existing individual and national efforts. Organizational interventions can be grouped as follows:

Technical Actions

- The Army could provide a data broker opt-out service to all servicemembers, civilians, and families either through commercially available providers or by creating an internal capability.
- Quantify, and ultimately block, third-party data collection, telemetry, and trackers on DODIN-A and Army-furnished devices (e.g., computers, smartphones). The Army could consider extending these blocking actions to personal devices used to access government resources (i.e., BYOD).
- The Army should ensure it is not integrating commercial data collection in its application software development processes via software development kits (SDKs).
- Expand the use of DS Logon and Login.gov to other government entities to minimize the use of commercial identity management companies like ID.me.

Policy Recommendations

- Army leaders should communicate the risks and observed impacts of publicly and commercially available data to inform state and federal policymakers with regard to data privacy legislation - regulating the collection, aggregation, sharing, and sale of personal information.
- Army leaders should also support research and advocacy on the establishment of state and/or federal laws that restrict or limit the sale of servicemember data.
- Army leaders should make informed recommendations to policymakers for the limiting of geo-location ad targeting and collection within a certain number of miles (to be determined) of any military installation, and remove the ability to target ads toward people with military-affiliated jobs/employers.

Doctrine

- The Army should continue to explicitly integrate and refine commercial PAI risk management, as acknowledged in ADP 3-13, into existing organizational policies and doctrine - including ADP 3-37 (Protection), ATP 3-13.3 (OPSEC), and others.
- The Army should (or advocate for the DoD to) persuade or advocate for data collection companies and data brokers to limit data collection in and around military bases and from military websites.
- Mandate that official operational communications (e.g., garrison operations, unit notifications) not occur on social media platforms. Soldiers and families should have official communications channels that are not susceptible to spoofing,

misinformation, or rely on them opting into commercial data collection by requiring an account on a private sector social media platform.

Personnel

- Develop a Home Use Program for privacy-enhancing technologies. The Army can (or advocate for the DoD) provide or subsidize personal privacy-enhancing technology services (e.g., VPNs, End-to-End Encryption (E2EE) personal email services, password managers) to all servicemembers, civilians, and families - either through commercially available providers or by standing up internal capabilities. Provide recommendations or infographics for securing home technology (e.g., routers, firewalls, cameras) as well as privacy-enhancing alternatives to UTS services like doorbell cameras and home security camera systems.
- Create a dedicated Army Red Team to assess friendly signatures created by Army personnel and operations available in PAI, similar to what is currently done in the OPSEC and cybersecurity fields.
- Develop an official messaging app/tool that reduces dependence on social media for family readiness groups, or other official communication mechanisms. This does not mean ceding the social media space but limiting it to proactive messaging rather than official information activities.

Army Contracting

- The Army should include privacy-enhancing requirements (anti-telemetry, limit sale or transfer of data, etc.) in its contracts with commercial service providers.
- The Army should review existing contracts for services and systems as potential sources of commercial data collection and develop contracting mechanisms to limit this collection.
- Review existing contracts related to medical providers, including investigating “seams” such as when soldier/family data is transferred to external providers through referrals. This also includes U.S. Family Health Plan coverage, which leverages private-sector partnerships for healthcare to Soldiers and families.

Awareness and Training Campaign

- The Army should research and maintain guides with specific recommendations for privacy-enhancing settings for personal devices and applications (e.g., Special Operations identity management smartcards[20]).

[20] USASOC Identity Management. https://www.soc.mil/IdM/publications/IdMpubs.html

- The Army should provide awareness training and best practices surrounding commercial data collection. This may include encouraging normative migration away from “freemium” services like free email providers and encouraging the development of best practices that minimize commercial data collection.
- The Army should develop case studies on Soldier data that have enabled malign action; these case studies could be integrated into individual training.
- Develop and support individual/household personal proactive measures by establishing best practices that are inculcated in PME and PCC, through formal organizations such as Soldier and Family Readiness Groups (SFRG), informal organizations like AUSA, and others.
- The Army should provide additional training/exercise resources to existing Red Teams (e.g., TSMO, 1st IO, USACE) to assess friendly signatures created by Army personnel and operations available as PAI.
- Add commercial data risk and vulnerability tools/assessments into all training exercises. Examples include:
    - Assess data vulnerabilities to wargame potential adversary actions against strategic, operational, and tactical organizational objectives. Leverage commercial data and tools to assess friendly vulnerabilities to avoid influence surprises.
    - Assess individual and commercial data vulnerabilities to assess key individuals' vulnerabilities to influence campaigns. Leveraging this kind of assessment for leaders to assess themselves will provide awareness that mitigates potential targeted campaigns.

Future Research

While there is significant reporting about privacy violations, this report only scratches the surface of the risks to the force from commercial data collection. There is still significant work to be done to better understand the risks to the formation as well as force projection capabilities and OPSEC concerns. This report concludes with recommendations for future research.

1. There are significant questions about the quality of collected data exchanged by data brokers. The quality and accuracy of the data purchased by the Duke team have not yet been confirmed by any Army or DoD organization. A critical future research agenda should include determining the accuracy of available data as well as the sources it is generated from.
2. Develop a research agenda to study emerging force protection issues surrounding privacy. Examples include biometric data collection, furthering understanding of

vulnerabilities, and assessing technical mitigation measures that can be implemented at scale.
3. Perform a study to assess commercial data collection (e.g., website analytics, device telemetry, cross-domain tracking) currently occurring on DODIN-A, to inform ARCYBER/G6 blocking efforts.
4. The Army should research future threats from the collection and use of non-standard data sources (e.g., vehicles, battlefield IOT, smart devices, biotech, healthcare devices, biometric identifiers, and other emerging areas of interest).
5. Develop a research agenda to understand whether individuals present in commercial datasets with recent life stressors are being targeted for malign influence.
6. Determine if commercial data be leveraged to impact (positively or negatively) force cohesion and readiness through cohesion corrosives (e.g., divisive issues around race, ethnicity, religion, or sexuality).
7. Determine how available commercial data informs emerging adversarial capabilities to target military servicemembers for blackmail or targeted influence campaigns.

Enclosures [available online]

Data Brokers and the Sale of Data on U.S. Military Personnel [link]