The New Insider Threat: How Commercially Available Data can be used to Target and Persuade

Jaclyn Fox

Introduction

By day, 21-year-old Jack Teixeira was a Massachusetts Air National Guard Member working on IT issues at Otis Air National Guard Base (Lamothe and Harris 2023). By night, he was the moderator of a racist, misogynistic, antisemitic Discord server threatening mass violence against marginalized communities and law enforcement officials (Harris and Oakford 2023). Notably, these two lives were not completely separate; on base, Teixeira's colleagues feared that he was showing signs of becoming a mass shooter (Lamothe and Harris 2023). However, when the airman was finally arrested it was for another form of insider threat: classified leaks.

1 Beginning in February 2022 and continuing until his arrest in April of 2023, Teixeira would leak hundreds of classified documents onto two Discord servers, amounting to one of the largest intelligence breaches in decades (Harris and Oakford 2023). Although Teixeira leaked documents that interested him – such as classified information about the Ukraine/Russia war, he also took requests from anonymous individuals within the server. For over a year Teixeira evaded detection despite numerous warning signs; on at least three separate occasions Teixeira's supervisors saw him looking at classified materials outside the scope of his position (Harris and Oakford 2023) and his colleagues repeatedly raised the alarm about disturbing behavior and fetishization of violence. Ultimately, however, the leaks were only discovered after another individual re-posted the materials which led to their spread across the internet.

JACLYN FOX

Dr. Jaclyn Fox is a postdoctoral fellow with the Army Educational Outreach Program (AEOP) affiliated with West Point's ACI. She obtained her PhD in international relations from American University where her dissertation focused on the spread of extremist narratives and mis/disinformation online and its relationship to actions offline. At West Point, she is continuing this stream of research along with an increased emphasis on the issues of insider threat and privacy.

This particular form of espionage may have been surprising to Teixeira's colleagues who witnessed his violent and erratic behaviors, however, indicators available in Teixeira's *online* life warned of this threat. Although not tracked by the U.S. military, servicemembers' online lives paint an intimate picture of their psyches. If an external actor is able to gain access to insiders' online lives this could render U.S. servicemembers and the U.S. military vulnerable to manipulation. In today's world access to this kind of data is unfortunately not a matter of "if" but "when" as commercial data brokers are already working to aggregate individuals' online rhetoric and offline behaviors to make inferences about their personalities, mental health, and ideological alignment, for targeting as consumers.

While existing literature examines the factors correlated with the perpetration of insider threat (Allen et al. 2023; Herbig 2017; Greitzer and Hohimer 2011; T. J. Thompson 2018; 2014; Shaw and Sellers 2015; Lenzenweger and Shaw 2022; Bedford and Van Der Laan 2021; Hugl 2010; Wilder 2017), it does not discuss how the newest element of technological innovation – mass commercial data collection – can be leveraged by actors seeking to undermine U.S. national security interests.[2] The current paper seeks to fill this gap asking: is it possible to use commercially available data to cultivate potential insider threats?

To understand the potential for using commercially available data in this manner, we develop a framework of "insider threat" correlates and motivations based on the available empirical literature. We then search the commercially available data for potential proxy variables that measure these factors.

2 Of note, a recent study by Duke examined the issue of commercial data collection and the U.S. military specifically; however, their findings were limited both in number of brokers and breadth of audience segments discussed (Sherman et al. 2023). We build on their important findings. Our analysis is essential as audience segments not originally scoped for U.S. military personnel may be cross-referenced or geo-located to military spaces allowing for a much wider range of "military" data available..

For this project, the commercial data utilized comes from a dataset aggregated by Microsoft's ad platform, Xandr, that was exposed during a recent investigation by the Markup. This comprehensive dataset contains 650,000 "audience segments" across 93 different data brokers highlighting the depth and breadth of commercial data collection activities (Keegan and Eastwood 2023).[3]

From our analysis we found that it is indeed possible to use commercially available audience segments to cultivate a list of individuals with the predispositions, recent life stressors, and insider access[4] making them vulnerable to engaging in acts against their organization. In other words, our findings suggest that available commercial data can be weaponized by external actors to sow discord within the U.S. armed forces and to cultivate a list of insiders with the predispositions and life stressors making them vulnerable to engaging in actions against their organizations. Importantly, nefarious outsiders in this instance are not limited to state actors or those with extensive funding. Rather, the cheap nature of this data (Sherman et al. 2023)[5] allows for nearly anyone with a credit-card – located across the globe – to weaponize this intimate knowledge about our nation's insiders.

Literature Review

Due to the immense risk posed by individuals with insider access turning against their organization, multiple studies have aimed to proactively identify those likely to engage in insider threat. This includes in-depth literature reviews highlighting the traits common to insider threats, empirical studies, analysis of specific cases, and even modelling[6] (Allen et al. 2023; Lenzenweger and Shaw 2022; Bedford and Van Der Laan 2021; Whitty 2021; Shaw and Sellers 2015; Philip Legg et al. 2013; Greitzer and Hohimer 2011). While the literature focuses on different aspects of this problem, there is wide agreement that behavioral and psychosocial indicators are essential to understanding who might engage in acts against their organization. Importantly, this body of literature is written with the idea in mind that organizations have access to these variables in order to model threat within their workers; however, in this paper we seek to understand if the same datapoints could be captured within the available commercial data and instrumentalized by external actors with mal intent.

3 See previuos note .

4 Numerous audience segments are available that both directly and through proxies identify individuals in the U.S. armed forces and working in the government.

5 A recent study by Duke researchers (2023) found that individually identifiable information on U.S. servicemembers and their families could be purchased for as little as $0.12 a record. At higher quantities of servicemembers the cost dropped to $0.01 per individual (Sherman et al. 2023).

6 Various researchers have worked to model potential insider threats using the datapoints discussed above (see: Allen et al. 2023 for a review). For organizations, managers often have access not only to technical details such as what an employee does online but their behavioral indicators as well when brought to the attention of HR departments. One such model used interviews with HR professionals to pinpoint various indicators that one may engage in insider threat behavior. These behaviors are joined with network monitoring to create an algorithm that may identify potential threats..

Who Engages in Insider Threat? Psychological Factors/Psychosocial Factors

The first category implicated in insider threat participation is psychological and social factors. Based on extensive empirical research, psychological factors such as the "big 5," e.g. agreeableness, conscientiousness, neuroticism, and "dark triad traits," i.e. narcissism, psychopathy, and Machiavellianism, are key to understanding those with the potential to engage in insider threat. Specific characteristics have also been implicated in these activities including anger, frustration, social isolation, entitlement, and lack of empathy (Allen et al. 2023; Shaw and Sellers 2015; Greitzer and Hohimer 2011; Hugl 2010). Of note, while all of these traits have been named in the literature, some may be more influential than others; Greitzer and Hohimer (2011) for instance proposed a weighting scheme in their model with items like disgruntlement and anger management weighing more heavily than items like absenteeism in predicting the potential for insider threat (Greitzer and Hohimer 2011, 32). On the psychosocial end, addiction and mental health disorders have also been associated with the perpetration of insider threat; however, it's essential not to stigmatize individuals for merely having a disorder. Rather, mental illness may be one data point that in conjunction with other data points highlights the need for further examination of an individual.

While many of the available studies speak of "insider threats" broadly, Allen et al. (2023) divide the group categorically into espionage/mass leaking, counterproductive work behaviors, and workplace violence. This delineation is especially useful as it allows for the discussion of psychological and psychosocial correlates both overall and in relation to specific threat types. Spies overall tend to be narcissistic, thrill seeking, grandiose, and desire both power and control (Allen et al. 2023; T. J. Thompson 2014; Wilder 2017). However, Allen et al. (2023) expose a slight demarcation between those who engage in traditional forms of espionage (e.g. Robert Hanssen) and mass leaking (e.g. Edward Snowden). While both tend to display narcissistic traits, the former also tends towards psychopathy and immaturity while the latter displays a grandiose need for recognition, belief that they are performing a "greater good", personal convictions, and disgruntlement (Allen et al. 2023, 21; T. J. Thompson 2018; Herbig 2017; T. J. Thompson 2014; Wilder 2017). In terms of workplace violence – such as the attack on Ft. Hood by Nidal Hasan, research specifies the role of a *narcissistic injury* (White 2021).

Regarding counterproductive work behaviors, dark triad traits are also implicated (Ellen et al. 2021; O'Boyle et al. 2012) as are the "big 5" attributes such as low agreeableness, low conscientiousness, and low emotional intelligence (Bowling et al. 2011; Ellen et al. 2021; Zhou, Meier, and Spector 2014). Lastly, high levels of aggression are also correlated with perpetration of counterproductive work behaviors (Galić and Ružojčić 2017; Kranefeld and Blickle 2022; Runge et al. 2020).

> **If an external actor is able to gain access to insiders' online lives this could render U.S. servicemembers and the U.S. military vulnerable to manipulation**

Finally, we turn to workplace violence. As workplace violence is a type of insider threat, it shares potential indicators with other forms including espionage. These indicators include aggression, feelings of injustice, perceived wrongdoing of organization, social isolation, financial issues, and grievances (Department of Homeland Security 2019). However, workplace violence has additional indicators relevant to the perpetration of mass violence more generally that may differ from other forms of insider threat. These could include access to and skill with weapons, substance abuse, suicidality/depression, homicidal fantasies, and specific preattack planning and preparation (Viñas-Racionero, Scalora, and Cawood 2021; Cybersecurity and Infrastructure Security Agency (CISA) 2020; Occupational Safety and Health Administration (OSHA) 2016). Of note, individuals like Teixeira demonstrate the interrelated nature of different forms of insider threat; although Teixeria maintained weapons and threatened violence he ended up betraying his service through mass classified leaks. Indicators such as narcissism and grievance against the government highlighted Teixeira's vulnerability to engaging in acts against the government broadly even if they didn't point to the specific type of threat.

In sum, all variations of insider threat tend to correlate with some form of dark triad trait (especially narcissism), elements of the big 5 personality inventory, and aggression. However, predispositions alone do not lead to engagement with insider threat behaviors; rather, these behaviors may intersect with underlying grievances and specific triggering events culminating in acts against one's organization. Below, we discuss this important interaction.

Stressors: Who Engages in Insider Threats?

Within every segment of the insider threat paradigm, underlying grievances and recent life stressors are highlighted. That is, it is not predispositions alone that make an individual engage in acts against their organization but predispositions in conjunction with life stressors. Stressors can include work-related issues – such as a poor person/organization fit, a "moral qualm" with one's organization, recent demotions or bad performance reviews (Hugl 2010, 96). Stressors could also be in one's personal life such as a recent divorce or high debt (Shaw and Sellers 2015). These "critical triggering events" interact with grievance and personal predispositions to raise the likelihood

of an individual's decision to turn against their organization (Shaw and Sellers 2015; Wilder 2017; Herbig 2017; Allen et al. 2023).

Of note, the U.S. military recognizes the role that life stressors play in the potential to engage in insider threat. To combat this, the Office of the Director of National Intelligence has initiated a process of continuous evaluation in which public records are constantly scanned to proactively identify potential stressors including arrest reports, credit scores, bankruptcies, and divorce (Marks 2014).[7]

Motivations: Who Engages in Insider Threat?

In addition to predispositions and stressors individuals must have a motivation for engaging in insider threat behaviors. For individuals who ultimately decide to act against their organization, motivations can be categorized in three ways: economic, ideological, and disgruntlement/revenge (Allen et al. 2023, 21). However, these categories are not mutually exclusive; rather individuals are often driven by multiple impulses. Robert Hanssen, for instance, claimed that he was driven to spy for Moscow based on financial incentives; however, he also "burned with resentment that he did not receive the respect and assignments he felt he deserved" (Baker 2023). Mass leakers, on the other hand, the newest form of insider threat – and the one most quickly growing – tend to be driven by notions of "fairness" or "what's right." They enjoy playing the expert and see themselves as helping (Allen et al. 2023, 21). This is an especially interesting finding and supports earlier research that many insiders are not approached by external actors but rather are driven to volunteer their services (Irvin and Charney 2014). New technology then may act to facilitate this underlying impulse as opposed to the number of individuals wishing to engage in this behavior actually increasing.

7 This is intended to be a supplement to security clearance investigations which occur every 5-10 years.

Of note, although neither financial nor ideological motivations are generally the sole motivating factor for involvement in insider threat actions (T. J. Thompson 2014; Allen et al. 2023, 22), finding proxies for both financial stress (e.g. large debts, bankruptcies, or gambling) and ideological positions (including moral qualms with organization) (T. J. Thompson 2018) in the commercial data would be useful to identify potentially vulnerable insiders. In the case of ideology for insider threat in the military, this could include proxies for trust in government, alignment with certain ideological positions (e.g. LGBTQ+ rights), or political alignment (especially if this is in opposition to the party in power).[8]

The last category of motivation revolves around disgruntlement/revenge against one's organization. This could take a multitude of forms including: viewing work as illegitimate or above one's pay grade, job insecurity, perception of poor person/organization fit, perceived injustices at work, unfair pay, or "psychological contract breaches" (Zhao et al. 2022; Berry, Ones, and Sackett 2007; Liao et al. 2021; Mackey et al. 2017; Allen et al. 2023). Some of these work-related grievances — such as poor person/organization fit — may also be elucidated through the ideological proxies discussed above.

As a final note, although the literature on insider threat pulls from different fields, including cyber security, information sciences, and behavioral sciences, different organization types (e.g. private sector vs military) and utilizes different methodologies, there is general agreement in the variables of interest for detecting potential insider threats. To detect potential threats one must look at individuals' predispositions – including psychological and psychosocial factors – stressful life events, and issues with the organization itself such as perceived ethical alignment (Hugl 2010, 94; Shaw and Sellers 2015; Greitzer and Hohimer 2011). It is these traits that we will focus on in the current study and aim to identify in the commercially available data.

As discussed, the key question for the current study is, would it be possible for an external actor to use commercially available data to cultivate a list of individuals with insider access who may be more likely to turn against their organization? The available literature paves the way for this process, allowing one to create a "framework" for insider threat perpetration and determining which variables one would look for in the data itself. However, before discussing the creation of this framework and its application, it is worthwhile to highlight the recent research on commercially available data more broadly.

Commercially Available Data

Recent research has implicated commercially available data in a variety of destructive

8 In terms of *violent* insiders, although ideological extremism may be present, radical beliefs are not sufficient for engagement with violence (e.g. Asal, Schulzke, and Pate 2014; McCauley and Moskalenko 2017). However, radical beliefs may shape the form the violence takes place in – such as the target choice (Allen et al. 2023).

outcomes for individuals. This includes reports of data brokers selling data of elderly people and those who are believed to be in cognitive decline so that they can be targeted with fraudulent content (Simmons and Sherman 2022) as well as a report by the Cyber Policy Program at Duke University revealing that data brokers advertise their lists of veterans and U.S. military personnel (Sherman 2021). Finally, research has pointed to numerous real-world implications of commercial data collection including people being denied medication (Szalavitz 2021), rejected for rental applications and home loans (Johnson 2023), or facing increasing barriers to government services (Donnan and Bass 2022).

In terms of military operations specifically, researchers at the Army Cyber Institute have recently begun digging into the commercial surveillance landscape in efforts to better understand what is revealed through commercial data collection. Investigative reports like those published at the Intercept, show detailed location identification through companies like Anomaly Six that can identify where specific individuals regularly visit and live (Biddle and Poulson 2022). Others, show how easy it is to dig deep into the data of millions of cell phones and identify a single military user or reveal nuclear secrets through online flashcard apps (S. A. Thompson and Warzel 2019; Postma 2021). Further reporting revealed the location of forward operating bases in remote areas through fitness apps like Strava (Hsu 2018). Finally, the battlefield in Ukraine is also revealing just how dangerous commercial devices are on the battlefield. The Russian military allegedly banned smartphone use by its soldiers back in 2019 (Nechepurenko 2019). This is an important development as Ukrainian forces are using social media posts to locate and attack Russian military and paramilitary forces (Burgess 2022).

While the above emphasizes the damage that commercial data collection can cause, it is worth discussing a few key points about data brokers *themselves* to better contextualize risk for the current study. The first point is the low-cost nature of this highly sensitive personally identifiable data. The Duke study, referenced above, showcased not only the ease of acquiring mass amounts of personally identifiable information but its cost-efficiency (Sherman et al. 2023). Posing as buyers from both the U.S. and Asia they were able to purchase bulk sensitive data on U.S. servicemembers and their families including health data, financial data, marital status, political affiliation, religious affiliation, children in home and interest in gambling for as little as $0.12 a record (Sherman et al. 2023, 29, 33, 37).[9] Further, the researchers were able to make these purchases without any verification of their identity.[10] This means that individuals with

9 The authors note that the cost per service member they were quoted ranged from $0.12 to $0.32 depending on how many records were being purchased at a time and the selection of variables. However, in greater numbers the per individual rate can drop to $0.01. Persistent location information was also available although the team did not purchase this.

10 Of note, verification practices varied by broker. However, for the ones that did verify buyer's identity, the process appeared to be about ensuring payment as opposed to risks posed by the sale (Sherman et al. 2023, 26). Further, one broker said that they required identity verification, but relented if the purchase was made by wire as opposed to credit card (Sherman et al. 2023, 26).

nefarious intentions, including foreign adversaries, or violent extremist groups, can easily purchase large quantities of personal information related to U.S. servicemembers and their families for blackmail, manipulation, or, as highlighted in the current study, to develop their own "insiders."

Additionally, even if brokers refuse certain entities – like foreign adversaries – the ability to purchase bulk sensitive data, the data itself is often perilously easy to hack or intercept. Recent high profile data hacks, such as Equifax and Marriott have demonstrated both this possibility as well as the interest (Del Valle 2024; Liptak 2018; Warren 2018). Further, researchers have showcased how a skilled individual could intercept sensitive information while it is being transmitted to data brokers from the apps that collect it. A report from the Consumer Council of Norway (2020) found that even the most sensitive information, like GPS coordinates, was being transmitted to data brokers from the apps in which it is collected on unencrypted connections, posing a serious security threat (Forbrukerrådet 2020, 103). That is, not only are apps *selling* (and sharing) users' sensitive data to brokers who aggregate and resell it, but the manner in which they 1) store this information[11] and 2) transmit it is so insecure that external actors can easily intercept the personal information.[12]

In the next section we lay out the research design for the current study, building on previous literature on commercial data collection as well as insider threat broadly, by mapping the potential for commercial data to be used to detect and exploit insider threats. We begin with a discussion of The Markup's investigation, followed by an analysis of the commercially available audience segments.[13]

> **Predispositions alone do not lead to engagement with insider threat behaviors; rather, these behaviors may intersect with underlying grievances and specific triggering events culminating in acts against one's organization.**

11 Dating apps in particular are a wealth of personal information including: persistent location, sexual orientation, religious affiliation, political ties, and drug use which have consistently been shown to lack appropriate data protections. Not only is the data sold to third parties but Tinder, Bumble, OkCupid, Grindr, and Facebook dating have all reported breaches (Rizvi and Fern 2021). In 2018, Grindr's data was breached exposing incredibly sensitive personal data including HIV status and GPS data – even if the user had proactively opted out of sharing the latter information (Ikeda 2020). While Grindr claimed to have solved the issue a follow-up report in 2019 found that this was not the case (Ikeda 2020).

12 Cybersecurity experts have also demonstrated the ease with which an external actor could pinpoint an individual's precise location by using trileration attacks on apps such as Tinder and Grindr. While Tinder reportedly fixed this error, Grindr was still vulnerable in follow-ups in 2016, 2018, and 2019 (Koch 2024; Ikeda 2020).

13 See https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you for the Markup's investigation.

Research Design

The purpose of the current study is to understand the depth and breadth of commercially available data being captured on individuals with insider access. Due to the wide-ranging nature of this data we focus on the key question: does data exist that would allow a nefarious outsider to identify individuals with classified access who may have the predispositions, recent life stressors, and motivation to engage in actions against their organization?

In June of 2023, researchers from The Markup uncovered a spreadsheet labelled "Data Marketplace – Buyer Overview" on the website of Microsoft's ad platform Xandr (formerly owned by AT&T). This database contained over 650,000 audience segments[9] across 93 data brokers and illustrates the troves of personal data being collected on individuals (Keegan and Eastwood 2023). For the current study, we analyzed the contents of this database with respect to identifying potential insider threats. The top 10 data brokers within the Xandr database are listed in Table 1.

Within the database, audience segments ranged from the mundane to the mortifying. Advertisers could target based on demographics such as location, relationship status, and age/sex as well as more sensitive topics such as the investigation's titular "heavy buyers of pregnancy tests." Additionally, advertisers could target lists of consumers based on psychological profiles such as the big 5 personality traits, reactivity to stress, and thrill-seeking behaviors as well as those working in the U.S. military or government. This data will prove key to identifying potential insider threats.

Table 1. Top 10 Data Brokers

Data Provider Name	n
Audiences by Oracle (BlueKai, Datalogix, AddThis)	132645
LiveRamp Data Store	82363
Grapeshot	73569
Nielsen Marketing Cloud	65610
Eyeota	53526
Factual Inc (Foursquare, location data)	29208
Oracle Customs (1st, BlueKai, Datalogix, AddThis)	26288
Adsquare (Data Provider)	15246
Dstillery	12630
Skydeo, Inc.	11972

**Note, data brokers are not synonymous with data providers. For instance, Experian is a very large data provider, however it is sold through brokers such as Oracle Customs and KBM Group.*

While consumers may have a vague notion as to the possibilities of data collection – phones' location data providing a timeline of places travelled, purchases made on credit cards aggregated, most are likely unaware of the scale of this collection, the ways in which it becomes tied together, or the ability of companies to use various pieces of information to create algorithms that make inferences about individuals including psychological profiling of personality traits.

14 An audience segment can be understood as a grouping of individuals for the purpose of targeted advertisement. Some of these segments are familiar and seemingly benign, e.g. individuals between 18 and 29, while others highlight the intimate details being collected on individuals. These could include individuals with specific mental health diagnoses, those who have insomnia due to chronic pain, and those who are caregivers for children.

Data and Methods

For the current study we wanted to understand the potential for misuse of the Xandr dataset by a nefarious actor. The research is guided by the question:

> **Can commercially available data be used to cultivate a list of potential insider threats for targeting?**

To investigate this possibility, we analyzed the dataset looking for the predispositions, life stressors, and motivations for engaging in insider threat behavior based on our literature review. When these factors are crossed with audience segments denoting individuals working for the U.S. military or government[15] this can create a list of potentially vulnerable individuals with insider access. While the available literature focuses on modeling potential insider threats for organizational security, we posit that these same characteristics can be used to reverse engineer a list of individuals with insider access who may be most vulnerable to engaging in actions against their organization. Thus, we were interested in whether the data could be used to identify relevant:

1. **Predispositions (e.g. psychological and psychosocial)**
2. **Life Stressors (e.g. divorce, financial stress)**
3. **Motivations (e.g. financial, ideological, work related)**

15 Numerous audience segments are available that both directly and through proxies identify individuals in the U.S. armed forces and working in the government.

Searching the Dataset

We began by developing a list of variables relevant to each of the above categories based on the literature review. For the psychological variables, for example, we created a list that included items such as "narcissism," "psychopathy," "thrill seeking," "conscientiousness," and "agreeableness." While some variables, such as "thrill seeking" had explicit audience segments in the dataset, others, such as narcissism, did not. We therefore expanded our search in two ways: word-based searches looking for synonyms that captured the same concept and broker-wide pulls on data brokers that were identified to capture other traits of interest.

In other words, we performed word-based searches of the Xandr dataset for 1) exact wording corresponding to specific variables implicated in the literature review, e.g. "narcissism" and 2) synonyms/related concepts to the identified variables, e.g. "self-involved". We then pulled all audience segments belonging to brokers that were identified as trafficking in any of the insider threat variables based on the initial word searches.

In this way, for each variable implicated in the literature, we searched for:

1. an **explicitly named audience segment,**
2. an **implicitly named audience segment** (i.e. named in an intuitive way that the researchers proactively searched for), and
3. an **audience segment covering the concept named in an idiosyncratic way** that did not appear in word-based searches but was sold by the same data broker trafficking in other segments of interest.

Table 2 outlines the key variables we sought in our analysis and relates them to the literature on insider threat perpetration.

Table 2. Insider Threat Framework

Category from Literature	Sub-Category from Literature	Exemplar Variables Sought from Database
Predispositions	Personality	• Dark Triad • Big 5 • Other Traits of Interest, e.g. anger, thrill seeking
	Psychosocial Traits	• Substance Abuse • Mental Health
	Demographics	• Gun Ownership
Stressors	Family	• Marriage/Divorce • Pregnancy • Terminal Illness • Recent Death • Frequent Moving
	Work	• Low Job Satisfaction • Moral Qualm with organization
Motivations	Financial	• Loans • Debt • Bankruptcy • Financial Changes • Gambling
	Ideological	• Immigration • LGBTQ+ • Abortion • Guns • Conspiracy • Trust in Institutions (media, banks, govt, social media) • Political Alignment
	Disgruntlement/ Revenge Against Organization	• Disengaged Worker • Overqualified Worker • Low Job Satisfaction • Ideological Misalignment with Organization (e.g. moral qualm)

> **For a small sum of money, external actors can purchase this dataset, allowing them to target thousands of potential insider threats.**

Ultimately, we developed an "insider threat framework" modeled off of the literature that seeks to proactively identify individuals who may engage in actions against their organization. The framework contains predispositions, stressors, and motivations for engaging in insider threat implicated in the empirical research.

Results

Our results show that the available commercial data can be used to identify individuals with insider access who may be more vulnerable to engaging in actions against their organizations. In fact, *all* of the data points from the Insider Threat framework in Table 2 are available for purchase from various data brokers. Below, we highlight key examples of available data by insider threat category; **Table 3 in the appendix lists exemplar data points for each framework item**.

Predispositions: Personality

As noted in the literature review, personality factors are a key correlate for willingness to engage in insider threat. From the available variables one could attain rough psychological profiles of current and former military members, cultivating lists of those with relevant (i.e., correlated with insider threat perpetration) traits. This has the potential to be a remarkably powerful – and low cost – way to target those with classified access who may be most likely to turn against their organization.

For example, the big 5 attributes, such as agreeableness (low), neuroticism (high), openness (low) and conscientiousness (low) are heavily implicated in the research on insider threat. All of these audience segments are available for purchase and can be cross-referenced with military members leading to a cohort of individuals with personality vulnerabilities and insider access.

VisualDNA Personality – US – Agreeableness – Lone Wolves

VisualDNA Personality – Personality – Agreeableness – Disinterested

VisualDNA Personality – US – Neuroticism – Trapped

Elements of the "dark triad" (i.e. narcissism, psychopathy, and Machiavellianism) are also linked to insider threat. Although these traits are not searchable within the commercial data directly, available audience segments (such as those listed below) can serve as proxies.

VisualDNA Mobile & App > Personality > UK > Agreeableness > Self Focused

VisualDNA Personality – Personality – Agreeableness – Control Seekers

Eyeota – US Experian – Psychographic / Attitudes – Self Concept – Dominating / Authoritarian

Eyeota – FI NDR – Insight360 – Values360 – 2 Self-centered and passive

Additionally, proxy variables can be found for anger/rage, poor stress tolerance, engagement with risky behavior/thrill seekers, and those with untapped grievances.

VisualDNA Personality – US – Neuroticism – Stress Reactors

VisualDNA > Personality > US > State of Mind > Frustrated

Eyeota – US Experian – Psychographic / Attitudes – Personal Views – Social Isolation

Eyeota – AU RDA Research – Consumer Profiles – Demo – General Attitudes – I generally get a raw deal out of life

Branded Data > Audigent > Programmatic Audio > Interest and Affinity > Thrill Seekers (BlueKai)

It is worth noting that just because individuals have this collection of traits, that does not mean that they will engage in insider threat behavior. As such, these categorizations should not be used to penalize individuals who are otherwise performing their duties. However, an adversary with access to a list of these individuals and malign intent could potentially cultivate insiders willing to turn against their organization.

Psychosocial Traits and Demographics

In addition to the psychological traits highlighted above, audience segments also illustrate individuals with demographics and psychosocial aspects that may increase their vulnerability to engaging in insider threat. Substance abuse has been implicated repeatedly in cases where individuals act against their organization, particularly with workplace violence. In addition, access to weapons is a key factor for individuals who go on to commit violence against their organization (Department of Homeland Security 2019). Exemplar segments are listed below.

Neustar AdAdvisor > AdAdvisor Political Audiences > Outlook > Gun Owners

Clickagy > Health > Addictions > Drugs

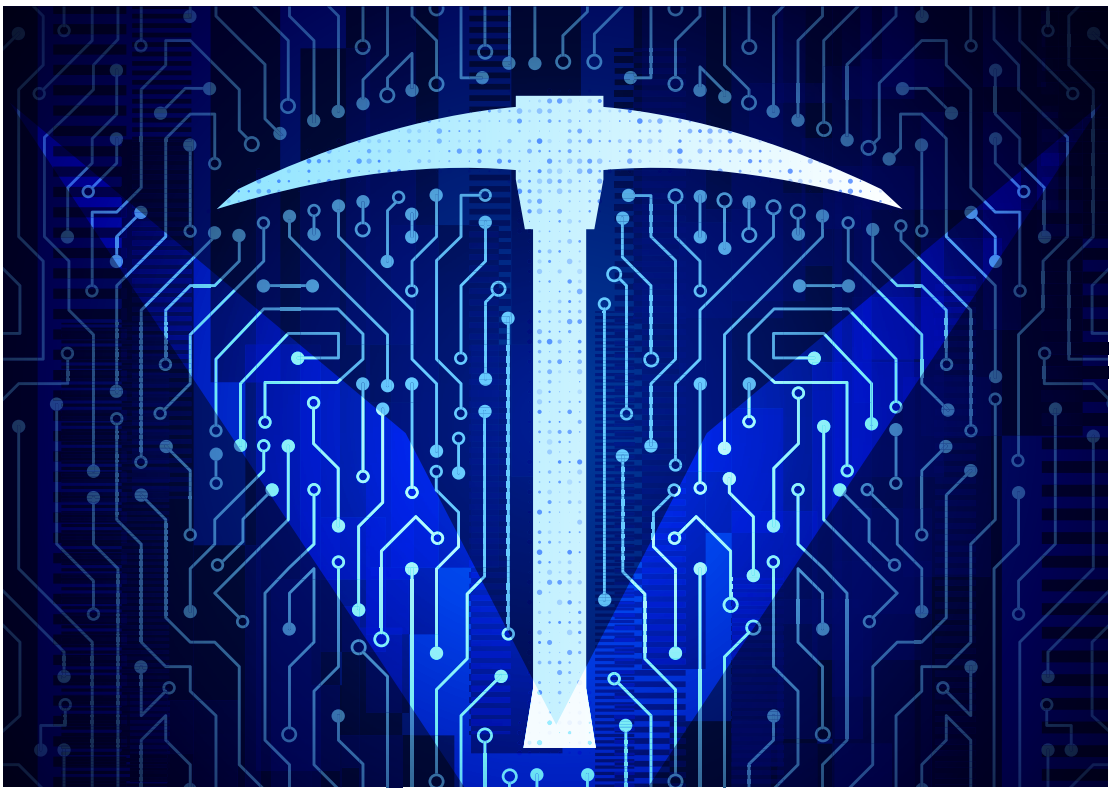
Skydeo > ConditionGraph > Health & Wellness > Lifestyle Indicators > Alcohol: Drink & Drive

Further, the data allows targeting of individuals with specific mental health diagnoses, such as PTSD, Anxiety, Depression, and Bipolar disorder. In addition, it highlights individuals who have been prescribed medication to treat these mental illnesses. It's important to note that mental health diagnoses in and of themselves do *not* indicate an increased propensity to engage in insider threat. It is thus important not to malign individuals with any mental health diagnosis or treatment. However, certain mental illnesses (such as those listed below) have been correlated with insider threat in the presence of additional factors. Additionally, if individuals use telemedicine or have their medications delivered by mail (both available audience segments) this could potentially open them up for tampering by malign actors.

Disease Propensity by Type > Anxiety Diagnosis (Adstra)

Eyeota – US Kantar – Health and Wellness – Conditions and Treatments – Post Traumatic Stress Disorder or Ptsd

Kantar > US > Custom > Use Any Rx Treatment for Depression



Stressors

After accounting for psychological and psychosocial predispositions and demographic characteristics, the next most important aspect of vulnerability to engaging in insider threat is experiencing recent life stressors. Research on previous cases of insider threat, in particular espionage, reveal individuals experiencing both professional and personal life stressors including "moral qualms" with their organization, financial difficulties, problems at home, and interpersonal issues at work. Reality Winner, for example, a former NSA contractor who leaked classified material to the online publication The Intercept, revealed moral qualms she was having both during her time in the Air Force and then at the NSA. In her home life, Winner experienced a major personal stressor right before leaking, losing her father with whom she had a close (but complicated) relationship (Stack 2022).

Audience segments are available to capture these varying personal and professional stressors including recent death, terminal diagnoses, those newly divorced, separated, married, or single, and those who feel disconnected from their work environment.

Adyoulikesa_bereavement

Consumer > Healthcare > Healthcare – Terminal Illness & Counseling

Branded Data > Media Source > Demographic > Family Composition > Marital Status > Recent Divorce (BlueKai)

Branded Data > Experian > Life Event > Recently Married > Last 3 Months (BlueKai)

Predictive Audience > Eyeota > Demo > US – Life Events – Expectant Mothers / Pregnancy

Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction

Motivations

In addition to *who* may be most vulnerable to engaging in insider threat actions, the commercially available data allows one to understand *why* these individuals would be willing to turn against their organizations. That is, audience segments are available for each of the three key categories of insider threat motivation: economic, ideological, and disgruntlement/revenge. These categories are not mutually exclusive; economic motivations, for instance, are often present but not the sole motivating factor for individuals who work against their organization (Allen et al. 2023, 22). Through the available data, however, one can ascertain which individuals may be motivated due to financial, ideological, or revenge-seeking needs.

Financials

Individuals with financial motivations to engage in insider threat can be ascertained through audience segments containing individuals with large loans, significant debt, gambling habits, and bankruptcies. Perhaps even more relevant are those with *recent financial changes* which includes individuals who saw their disposable income decrease by over 75% in the last 5 years. Although it is not clear how much these individuals still have, the perceived relative deprivation could be a major financial motivator. Essentially, a malign actor could target individuals involved in military or government work who hold large debts, are gambling addicts, or are seeking immediate loans and offer a way out of their financial struggles.

Ideological

A second category of motivation to engage in insider threat is related to ideological beliefs. Within the commercial data there are audience segments that target individuals on both sides of contentious issues including: abortion (pro-life/pro-choice), support for gun control vs support for the 2nd amendment, immigration issues, views on the LGBTQ+ community, and others. These ideological buckets serve the dual purpose of identifying individuals with an ideological motive for "revenge" against an organization as well as formulating potential targets lists. Audience segments also capture those who support conspiratorial and anti-government views and individuals' overall political alignment.

Targeting individuals who consume conspiratorial media or those who self-identify as doomsday preppers and "patriots seeking security" — all available audience segments — would be especially useful in the case of insider threat within the military or government. In addition, targeting individuals by support for (or rejection of) politicians like former President Trump could identify those with military/government related ideological grievance.

In sum, ideological audience segments can be utilized to identify individuals who may be anti-government (e.g., self-designated "patriots" or those who don't trust institutions), those who have moral qualms with the organization (e.g., with actions being taken by the military) or misalignment on political issues such as trans rights. Of note, potential moral qualms shift over time; when Trump was in office "Trump Resistors" may have experienced moral qualms, while self-described "patriots" may feel misaligned under Biden.

Work Resentment

A third key motivator for engaging in insider threat is disgruntlement/desire for revenge against one's organization. This could be due to a problematic individual/organization relationship, available through audience segments such as low job satisfaction or disengagement from work. Although Teixeira showed warning signs before and after his entry into the Air National Guard, it was after being disciplined for looking at classified materials that colleagues noted a marked change in his personality. They reported Teixeira seemed like a "completely different person" after being "admonished" and worried that he would "do something drastic" (Lamothe and Harris 2023). Of note, fears at the time were that Teixeira would become an active shooter not a mass leaker; however, this emphasizes the inter-connected nature of various kinds of insider threat perpetration.

In terms of military members specifically, ideological views that lead to a "moral qualm" with the government or military are especially relevant. These could include views on hot button issues such as transgender individuals in the military, the role of the military in certain conflicts, or the very legitimacy of the U.S. government as discussed above.

Conclusion

This paper has demonstrated that commercially available data contains proxy variables which can identify individuals' insider access as well as whether they contain the predispositions and motivations for engaging in actions against their organization. For a small sum of money, external actors can purchase this dataset, allowing them to target thousands of potential insider threats. While not all individuals in the dataset will be potential threats, this data presents a low cost, low risk and potentially high reward endeavor by nefarious actors; only one individual on a list of potentially hundreds or thousands would need to "bite" to be worthwhile. Further, due to the low cost of commercially available data, the kinds of actors able to engage in this effort are broadened. Malicious state actors could purchase the data; however, nonstate actors, and even individuals are able to as well.

Through an analysis of the literature on insider threat and/or a close examination of the available information on previous perpetrators of espionage, mass leaking, and treason, one may curate a list of military members with the common predispositions and recent life stressors that make individuals vulnerable to engaging in insider threat.

Further, once this list is crafted, malign actors could use the available commercial data to understand what would motivate specific individuals to work against their organization and how to best approach them. Essentially, the available commercial data allows for the cultivation of a list potentially containing the next Chelsea Manning or Reality Winner, compiling all individuals possessing the characteristics common to mass leakers who also have classified access.

At the moment of this writing, all of the data collection and selling/sharing practices described above are legal[16] in the U.S. context.[17] This includes when the data is being purchased by individuals who may (or may not) have nefarious intentions, U.S. law enforcement officials,[18] the U.S. intelligence community, or foreign adversaries. Further, with individual records on sale for mere pennies, this data is accessible to nearly anyone with a credit card (Forbrukerrådet 2020, 43). Recently, however, legislators have begun to fight back, pushing for new bills that would limit the ability of data brokers to conduct unfettered trade in Americans' personally identifiable information.[19]

In February of this year, the Biden administration issued an Executive Order calling for the ban of data brokers' ability to sell U.S. bulk sensitive data to "countries of concern,"[20] such as Iran, China, Russia, and North Korea (Biden 2024). These particular transactions are especially concerning due to the potential for blackmail of Americans including U.S. servicemembers and government personnel (McKenna 2024). The EO tasked the Department of Justice with constructing new regulations to prevent the bulk transfer of this data to the aforementioned countries and to empower other federal agencies with stopping the transfer of specific health and genomic data (McKenna 2024; Brown, Chin-Rothmann, and Brock 2024).

These agencies are stepping up in earnest. In March of 2024 the House passed a bill that would ban the sale of sensitive information to foreign adversaries (Feiner

16 While this may seem surprising due to existing laws such as HIPPA, it's important to note that this (and other existing) privacy legislation is entity based. That is, entities like *hospitals* cannot share an individual's health information, however *apps* are under no such legal constraint (Forbrukerrådet 2020, 11).

17 It's worth noting that while this form of data collection and dissemination may be legal in the U.S., in other markets it operates on a shakier foundation. Per a 2020 report by the Consumer Council of Norway, the authors found that much of the data transmission was actually illegal per the General Data Protection Regulation (GDPR) (Forbrukerrådet 2020, 6).

18 In the 2018 landmark court case *Carpenter*, the courts found that law enforcement needed to obtain a warrant in order to access an individual's persistent location data. However, there is a loop hole in the Fourth Amendment protection; when individuals "give consent" to apps to access this data and it is bought and sold through data brokers, law enforcement can then legally purchase the data circumventing the warrant requirement (Brennan, Coulthart, and Nussbaum 2023, 86). The proposed "Fourth Amendment is Not For Sale Act" would explicitly prohibit the sale of this data to the U.S. government and require a court order to obtain GPS data (Chin-Rothmann 2023, 26).

19 At the federal level, multiple bills are being put forth with the aim of curbing data collection and sharing. Many of the propositions would give U.S. citizens the same protections held under the European Union's GDPR which includes the right to view and change information held by brokers (Chin-Rothmann 2023, 25).

20 While discussions of banning particular apps, like TikTok due to its Chinese ownership, dominates the newsfeed, China could just as easily access this information by purchasing it (and much more) from data brokers.

2024) and the Consumer Financial Protection Bureau began debating new regulations that would require data brokers to comply with Fair Credit Reporting Act. In essence, treating them as "consumer reporting agencies" which would ban sharing of certain kinds of data unless there was a "specific purpose outlined in the law" (Del Valle 2024).

Importantly, however, the executive order does not contain information on how brokers must "aggregate, process, store, and share sensitive information" with U.S. entities (Brown, Chin-Rothmann, and Brock 2024) nor does it prohibit the sharing/selling of sensitive information to countries which are not designated as "concerning". This creates an opening for other individuals to buy and resell the information to countries of concern or for these countries to acquire the data through other means such as hacking or intercepting data transmissions. That is, as long as the industry persists, so will the threat.[21]

In the months and years ahead, it will be essential to continue pushing for controls on the collection and dissemination of Americans' personal data. This demands both a legislative and research response. On the legislative end, future bills must work to curtail not only sales to "countries of concern" but the collection and dissemination of this data more broadly. For as long as the industry persists, the data will be at risk of falling into nefarious hands. On the research end, a robust research agenda must be developed and enacted to understand the varying sources of this data, its accuracy, and how/when/by whom this data is being acquired and utilized.

On a final note, it's worth mentioning that due to the nature of this data government entities could purchase it as well in an effort to stem potential insider threats. In fact, in many ways this data is more comprehensive than that which currently underwrites efforts like continuous monitoring. Audience segments include the stressors discussed above as well as comprehensive psychological profiles that tap into individuals' "online lives." However, we argue that U.S. citizens – including service members and their families – would be better served by developing policies to keep this data from being collected, aggregated, and sold indiscriminately. The potential for misuse outweighs positive outcomes.

21 While the EO did set in motion some important legislative changes, McKenna (2024) argues that the order's "larger significance lies in its stated rationale for why the U.S. needs such an order to protect people's sensitive data in the first place." That is, while the EO does not demand a large-scale recalibration of the data broker industry it serves the integral role of informing the public about the "staggering" amount of data that is currently up for sale.

REFERENCES

Allen, Matt, Kat Parsons, Tin Nguyen, and Lauren Zimmerman. 2023. "Examining Best Practices in Threat Assessment from an Insider Threat Perspective." National Counterterrorism Innovation, Technology, and Education Center. https://www.unomaha.edu/ncite/_files/insider-threat-and-threat-assessment-literature-review-website-version96.pdf.

Baker, Peter. 2023. "Robert Hanssen, F.B.I. Agent Exposed as Spy for Moscow, Dies at 79." *The New York Times*, June 5, 2023, sec. U.S. https://www.nytimes.com/2023/06/05/us/robert-hanssen-spy-dead.html.

Bedford, Justine, and Luke Van Der Laan. 2021. "Operationalising a Framework for Organisational Vulnerability to Intentional Insider Threat: The OVIT as a Valid and Reliable Diagnostic Tool." *Journal of Risk Research* 24 (9): 1180–1203. https://doi.org/10.1080/13669877.2020.1806910.

Berry, Christopher M., Deniz S. Ones, and Paul R. Sackett. 2007. "Interpersonal Deviance, Organizational Deviance, and Their Common Correlates: A Review and Meta-Analysis." *Journal of Applied Psychology* 92 (2): 410–24. https://doi.org/10.1037/0021-9010.92.2.410.

Biddle, Sam, and Jack Poulson. 2022. "American Phone-Tracking Firm Demo'd Surveillance Powers by Spying on CIA and NSA." The Intercept. April 22, 2022. https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/.

Biden, Joseph R. 2024. "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The White House. February 28, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

Bowling, Nathan A., Gary N. Burns, Susan M. Stewart, and Melissa L. Gruys. 2011. "Conscientiousness and Agreeableness as Moderators of the Relationship Between Neuroticism and Counterproductive Work Behaviors: A Constructive Replication: Personality and CWBS." *International Journal of Selection and Assessment* 19 (3): 320–30. https://doi.org/10.1111/j.1468-2389.2011.00561.x.

Brennan, Shelby, Stephen Coulthart, and Brian Nussbaum. 2023. "The Brave New World of Third Party Location Data." *Journal of Strategic Security* 16 (2): 81–95. https://doi.org/10.5038/1944-0472.16.2.2070.

Brown, Evan, Caitlin Chin-Rothmann, and Julia Brock. 2024. "Exploring the White House's Executive Order to Limit Data Transfers to Foreign Adversaries," February. https://www.csis.org/analysis/exploring-white-houses-executive-order-limit-data-transfers-foreign-adversaries.

Burgess, Matt. 2022. "Their Photos Were Posted Online. Then They Were Bombed." *Wired UK*, August 26, 2022. https://www.wired.co.uk/article/wagner-group-osint-russia-ukraine.

Chin-Rothmann, Caitlin. 2023. "Surveillance for Sale," CSIS Strategic Technologies Program, , June, 1–55.

Cybersecurity and Infrastructure Security Agency (CISA). 2020. "ISC Violence in the Federal Workplace Guide | CISA." December 17, 2020. https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide.

Del Valle, Gaby. 2024. "The CFPB Wants to Rein in Data Brokers - The Verge." The Verge. April 15, 2024. https://www.theverge.com/2024/4/15/24131354/cfpb-data-brokers-fair-credit-reporting-act.

Department of Homeland Security. 2019. "Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence." https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorismtargeted- violence.pdf.

Donnan, Shawn, and Dina Bass. 2022. "How Did ID.Me Get Between You and Your Identity?" *Bloomberg.Com*, January 20, 2022. https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper.

Ellen, B. Parker, Katherine C. Alexander, Jeremy D. Mackey, Charn P. McAllister, and Jack E. Carson. 2021. "Portrait of a Workplace Deviant: A Clearer Picture of the Big Five and Dark Triad as Predictors of Workplace Deviance." *Journal of Applied Psychology* 106 (12): 1950–61. https://doi.org/10.1037/apl0000880.

Feiner, Lauren. 2024. "House Passes Bill to Prevent the Sale of Personal Data to Foreign Adversaries." The Verge. March 20, 2024. https://www.theverge.com/2024/3/20/24106991/house-data-broker-foreign-adversaries-bill-passes.

Forbrukerrådet. 2020. "OUT OF CONTROL: How Consumers Are Exploited by the Online Advertising Industry." The Consumer Council of Norway. https://www.forbrukerradet.no/out-of-control/.

Galić, Zvonimir, and Mitja Ružojčić. 2017. "Interaction between Implicit Aggression and Dispositional Self-Control in Explaining Counterproductive Work Behaviors." *Personality and Individual Differences* 104 (January): 111–17. https://doi.org/10.1016/j.paid.2016.07.046.

Greitzer, Frank L., and Ryan E. Hohimer. 2011. "Modeling Human Behavior to Anticipate Insider Attacks." *Journal of Strategic Security* 4 (2): 25–48. https://doi.org/10.5038/1944-0472.4.2.2.

Harris, Shane, and Samuel Oakford. 2023. "Jack Teixeira Got Security Clearance despite History of Violent Threats." Washington Post. December 11, 2023. https://www.washingtonpost.com/national-security/2023/12/11/jack-teixeira-discord-leaks/.

Herbig, Katherine L. 2017. "The Expanding Spectrum of Espionage by Americans, 1947-2015." https://apps.dtic.mil/sti/citations/AD1040851.

Hsu, Jeremy. 2018. "The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data." *Wired*, January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Hugl, Ulrike. 2010. "The Malicious Insider Problem: An Integrated View on Individual, Organizational and Contextual Influencing Factors." In , 93–101. Thessaloniki, Greece.

REFERENCES

Ikeda, Scott. 2020. "Many of the Major Dating Apps Are Leaking Personal Data to Advertisers." CPO Magazine (blog). January 30, 2020. https://www.cpomagazine.com/data-privacy/many-of-the-major-dating-apps-are-leaking-personal-data-to-advertisers/.

Irvin, John a, and David L. Charney. 2014. "Stopping the Next Snowden." *POLITICO Magazine*. March 25, 2014. https://www.politico.com/magazine/story/2014/03/stopping-next-edward-snowden-105004.

Johnson, Khari. 2023. "Algorithms Allegedly Penalized Black Renters. The US Government Is Watching." *Wired*, January 16, 2023. https://www.wired.com/story/algorithms-allegedly-penalized-black-renters-the-us-government-is-watching/.

Keegan, Jon, and Joel Eastwood. 2023. "From 'Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You – The Markup." June 8, 2023. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

Koch, Richie. 2024. "How to Protect Your Privacy on Dating Apps | ProtonVPN." Proton VPN Blog. February 12, 2024.

Kranefeld, Iris, and Gerhard Blickle. 2022. "Disentangling the Relation between Psychopathy and Emotion Recognition Ability: A Key to Reduced Workplace Aggression?" *Personality and Individual Differences* 184 (January): 111232. https://doi.org/10.1016/j.paid.2021.111232.

Lamothe, Dan, and Shane Harris. 2023. "Accused Leaker Teixeira Was Seen as Potential Mass Shooter, Probe Finds." *Washington Post*, December 23, 2023. https://www.washingtonpost.com/national-security/2023/12/22/teixeira-investigation-active-shooter-threat/.

Lenzenweger, Mark F., and Eric D. Shaw. 2022. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." *Counter-Insider Threat Research and Practice* 1 (1).

Liao, Zhenyu, Hun Whee Lee, Russell E. Johnson, Zhaoli Song, and Ying Liu. 2021. "Seeing from a Short-Term Perspective: When and Why Daily Abusive Supervisor Behavior Yields Functional and Dysfunctional Consequences." *Journal of Applied Psychology* 106 (3): 377–98. https://doi.org/10.1037/apl0000508.

Liptak, Andrew. 2018. "Hackers Accessed More Personal Data from Equifax than Previously Disclosed - The Verge." The Verge. February 11, 2018. https://www.theverge.com/2018/2/11/17001046/equifax-hack-personal-data-tax-identification-numbers-email-addresses-drivers-licenses-cybersecurity.

Mackey, Jeremy D., Rachel E. Frieder, Jeremy R. Brees, and Mark J. Martinko. 2017. "Abusive Supervision: A Meta-Analysis and Empirical Review." *Journal of Management* 43 (6): 1940–65. https://doi.org/10.1177/0149206315573997.

Marks, Joseph. 2014. "Aiming to Stop the next Snowden." POLITICO. September 17, 2014. https://www.politico.com/story/2014/09/pentagon-edward-snowden-111030.

McKenna, Anne Toomey. 2024. "Biden Executive Order on Sensitive Personal Information Does Little for Now to Curb Data Market – but Spotlights the Threat the Market Poses." The Conversation. March 2, 2024. http://theconversation.com/biden-executive-order-on-sensitive-personal-information-does-little-for-now-to-curb-data-market-but-spotlights-the-threat-the-market-poses-224702.

Nechepurenko, Ivan. 2019. "Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces." *The New York Times*, February 19, 2019, sec. World. https://www.nytimes.com/2019/02/19/world/europe/russia-military-social-media-ban.html.

O'Boyle, Ernest H., Donelson R. Forsyth, George C. Banks, and Michael A. McDaniel. 2012. "A Meta-Analysis of the Dark Triad and Work Behavior: A Social Exchange Perspective." *Journal of Applied Psychology* 97 (3): 557–79. https://doi.org/10.1037/a0025679.

Occupational Safety and Health Administration (OSHA). 2016. "Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers (OSHA 3148-06R 2016)." U.S. Department of Labor: OSHA. https://www.osha.gov/sites/default/files/publications/OSHA3148.pdf.

Philip Legg, Nick Moffat, Jason R.C. Nurse, Jassim Happa, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. 2013. "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 4 (4): 20–37. https://doi.org/10.22667/JOWUA.2013.12.31.020.

Postma, Foeke. 2021. "US Soldiers Expose Nuclear Weapons Secrets Via Flashcard Apps." Bellingcat. May 28, 2021. https://www.bellingcat.com/news/2021/05/28/us-soldiers-expose-nuclear-weapons-secrets-via-flashcard-apps/.

Rizvi, Hur-Ali, and Melinda Fern. 2021. "Data Privacy and Dating Apps: Dangerous Implications for the LGBTQ+ Community." *Foundation for a Human Internet* (blog). June 30, 2021. https://medium.com/humanid/data-privacy-and-dating-apps-dangerous-implications-for-the-lgbtq-community-345b70643491.

Runge, J. Malte, Jonas W.B. Lang, Ingo Zettler, and Filip Lievens. 2020. "Predicting Counterproductive Work Behavior: Do Implicit Motives Have Incremental Validity beyond Explicit Traits?" *Journal of Research in Personality* 89 (December): 104019. https://doi.org/10.1016/j.jrp.2020.104019.

Shaw, Eric, and Laura Sellers. 2015. "Application of the Critical-Path Method to Evaluate Insider Risks." I*nternal Security and Counterintelligence* 59 (2): 1–8.

Sherman, Justin. 2021. "Data Brokers Are Advertising Data on U.S. Military Personnel." Lawfare. August 23, 2021. https://www.lawfaremedia.org/article/data-brokers-are-advertising-data-us-military-personnel.

Sherman, Justin, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan. 2023. "Data Brokers and the Sale of Data on U.S. Military Personnel." Duke University. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

Simmons, Alistair, and Justin Sherman. 2022. "Data Brokers, Elder Fraud, and Justice Department Investigations." Lawfare. July 25, 2022. https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations.

REFERENCES

Stack, Megan K. 2022. "Opinion | She Tried to Resist and Found Herself Alone." *The New York Times*, December 6, 2022, sec. Opinion. https://www.nytimes.com/2022/12/06/opinion/reality-winner.html.

Szalavitz, Maia. 2021. "The Pain Was Unbearable. So Why Did Doctors Turn Her Away?" *Wired*, August 11, 2021. https://www.wired.com/story/opioid-drug-addiction-algorithm-chronic-pain/.

Thompson, Stuart A., and Charlie Warzel. 2019. "Opinion | Twelve Million Phones, One Dataset, Zero Privacy." *The New York Times*, December 19, 2019, sec. Opinion. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

Thompson, Terence J. 2014. "Toward an Updated Understanding of Espionage Motivation." *International Journal of Intelligence and CounterIntelligence* 27 (1): 58–72. https://doi.org/10.1080/08850607.2014.842805.

——. 2018. "A Psycho-Social Motivational Theory of Mass Leaking." *International Journal of Intelligence and CounterIntelligence* 31 (1): 116–25. https://doi.org/10.1080/08850607.2017.1374800.

Viñas-Racionero, Rosa, Mario J. Scalora, and James S. Cawood. 2021. "Workplace Violence Risk Instrumentation: Use of the WAVR-21 V3 and the CAG." In *International Handbook of Threat Assessment*, by Rosa Viñas-Racionero, Mario J. Scalora, and James S. Cawood, edited by J. Reid Meloy and Jens Hoffmann, 522–35. Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0030.

Warren, Tom. 2018. "Marriott Reveals Massive Database Breach Affecting up to 500 Million Hotel Guests." The Verge. November 30, 2018. https://www.theverge.com/2018/11/30/18119403/marriott-database-breach-starwood-hotels.

White, Stephen G. 2021. "Workplace Targeted Violence: Assessment and Management in Dynamic Contexts." In *International Handbook of Threat Assessment*, by Stephen G. White, edited by J. Reid Meloy and Jens Hoffmann, 107–35. Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0006.

Whitty, Monica T. 2021. "Developing a Conceptual Model for Insider Threat." *Journal of Management & Organization* 27 (5): 911–29. https://doi.org/10.1017/jmo.2018.57.

Wilder, Ursula M. 2017. "The Psychology of Espionage." *Studies in Intelligence* 61 (2): 19–36.

Zhao, Lijing, Long W. Lam, Julie N. Y. Zhu, and Shuming Zhao. 2022. "Doing It Purposely? Mediation of Moral Disengagement in the Relationship Between Illegitimate Tasks and Counterproductive Work Behavior." *Journal of Business Ethics* 179 (3): 733–47. https://doi.org/10.1007/s10551-021-04848-7.

Zhou, Zhiqing E., Laurenz L. Meier, and Paul E. Spector. 2014. "The Role of Personality and Job Stressors in Predicting Counterproductive Work Behavior: A Three-way Interaction." *International Journal of Selection and Assessment* 22 (3): 286–96. https://doi.org/10.1111/ijsa.12077.

Table 3. Insider Threat Framework with (selected) Proxy Variables from Commercial Data

Category	Sub-Category	Exemplar Variables	Exemplar Variables
Predispositions	Personality	Dark Triad	• Eyeota – FI NDR – Insight360 – Values360 – 2 Self-centered and passive • VisualDNA Mobile & App > Personality > UK > Agreeableness > Self Focused
		Big 5	• VisualDNA Personality – US – Agreeableness – Lone Wolves • VisualDNA Personality – US – Neuroticism – Trapped • VisualDNA Personality – US – Conscientiousness – Spontaneous Coasters
		Other Traits of Interest	• Eyeota – US Experian – Psychographic / Attitudes – Self Concept – Dominating / Authoritarian • VisualDNA Personality – Personality – Agreeableness – Control Seekers • VisualDNA Personality – US – Neuroticism – Stress Reactors • Eyeota – US Experian – Psychographic / Attitudes – Personal Views – Social Isolation • Eyeota – AU RDA Research – Consumer Profiles – Demo – General Attitudes – I generally get a raw deal out of life • Branded Data > Connexity > CNX Lifestyle > The Adrenaline Junkie (BlueKai)
	Psychosocial Traits	Substance Abuse	• Skydeo > ConditionGraph > Health & Wellness > Lifestyle Indicators > Alcohol: Drink & Drive
		Mental Health	• Kantar > US > Custom > Use Any Rx Treatment for Depression • Eyeota – US Kantar – Health and Wellness – Conditions and Treatments – Post Traumatic Stress Disorder or Ptsd
	Demographics	Gun Ownership	• Neustar AdAdvisor > AdAdvisor Political Audiences > Outlook > Gun Owners
Stressors	Family	Marriage/Divorce	• Branded Data > Media Source > Demographic > Family Composition > Marital Status > Recent Divorce (BlueKai) • Branded Data > Experian > Life Event > Recently Married > Last 3 Months (BlueKai)
		Pregnancy	• Predictive Audience > Eyeota > Demo > US – Life Events – Expectant Mothers / Pregnancy
		Terminal Illness	• Consumer > Healthcare > Healthcare – Terminal Illness & Counseling
		Recent Death	• Adyoulikesa_bereavement
		Frequent Moving	• Eyeota – DE Schober – Living Environment – Moving Frequency – High Fluctuation
	Work	Low Job Satisfaction	• Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction
		Moral Qualm with organization	
Motivations	Financial	Loans	• Branded Data > Gravy Analytics > In-Market > In-Market Payday Loans (BlueKai)
		Debt	• Zipline Estimated Household Debt Level $75,000 +
		Bankruptcy	• Companies In-Market for Goods & Services > Financial Services – Bankruptcy & Insolvency (Adstra)
		Financial Changes	• Powerlytics Stirista Fusion > Income Changes > Disposable Income 5 Year Percent Change > Disposable Income Decrease 75+% in the Last 5 Years
		Gambling	• Clickagy > Health > Addictions > Gambling

Table 3. Insider Threat Framework with (selected) Proxy Variables from Commercial Data *(Cont'n)*

Category	Sub-Category	Exemplar Variables	Exemplar Variables
Motivations	Ideological	Immigration	• Infogroup > B2C > Politics > Issues > Immigration > Mexican Border Wall > Supporters – Co-op Sourced
		LGBTQ+	• Social Profiles by Type > Lesbian/Gay/Bisexual/Transgender (LGBT) Supporters (Adstra) • Infogroup > B2C > Politics > Issues > Social > Transgender Bathroom Rights > Opponents – Co-op Sourced
		Abortion	• Infogroup > B2C > Politics > Issues > Social > Abortion Rights > Pro Life Supporter – Co-op Sourced • Infogroup > B2C > Politics > Issues > Social > Abortion Rights > Pro Choice Supporter – Co-op Sourced
		Guns	• Social Profiles by Type > 2nd Amendment Supporters (Adstra) • Social Profiles by Type > Gun Control Supporters (Adstra) • Infogroup > Consumer > US Politics > Issues & Advocacy > Registered Gun Owner Concealed Permit
		Conspiracy	• Audiences by Oracle > Consumer Packaged Goods (CPG) > Datalogix (DLX) Purchase-Based > BuyStyles > Non-GMO (BlueKai) • Consumer > Media > Right Wing Blogs – Conspiracy Theories (Dstillery) • Branded Data > Gravy Analytics > Lifestyle > Survivalist Prepper Interest (BlueKai)
		Trust in Institutions (media, banks, govt, social media)	• Neustar AdAdvisor > Attitudes > > Uncomfortable trusting money to a Bank • Fluent > TS Modeled > COVID 2021 > Not Planning to Get Vaccine > Dont Trust Vaccines • Infogroup > Consumer > US Politics > Media Consumption > News Source–Most Trusted Source – FOX • Infogroup > Consumer > US Politics > Media Consumption > News Source–Most Trusted Source – MSNBC • Nielsen Movies – Entertainment Behaviors – Trust Social Media Posts from Friends/Family (NRG) (Exelate) • Eyeota – FI NDR – Insight360 – Values360 – 4 Patriots seeking security • L2 Voter Data > Individual Demographics > Parties Description > Patriot
		Political Alignment	• Branded Data > ALC > Aristotle Political Precision (US) > Political Affiliation by Party > Conservative-Very Conservative (BlueKai) • Affluent Consumers by Political Affiliation > Democrat (Adstra) • Political Affiliations :: Trump Resistor :: (All) • Political Affiliations :: Trump Supporter :: (All)
	Disgruntlement/ Revenge Against Organization	Disengaged Worker	• VisualDNA > Personality > UK > Resourcefulness > Disengaged Workers
		Overqualified Worker	• VisualDNA > Personality > US > Resourcefulness > Overqualified Workers
		Low Job Satisfaction	• Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction
		Ideological Misalignment with Organization (e.g. moral qualm)	• See ideology section and political alignment