2023 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

ETHICS & OSINT SCORECARD

OVERVIEW

Open-source intelligence (OSINT), defined as intelligence produced from publicly available information, is increasingly used by private sector entities for a variety of purposes, such as to protect their brand, return-on-investment, employees, or to gain advantage over market competitors. Furthermore, corporate use of OSINT is rapidly evolving, and capabilities are increasing, due to technological advances in fields such as data science and artificial intelligence. Private sector entities' use of OSINT is bound by federal, state, and local law; however, they face far less restrictions than their government counterparts—and there are no generally-accepted ethical guidelines for how the private sector should collect, analyze, and obtain such information.*

This Scorecard is intended to aid in addressing these concerns and is designed to assist corporate decision-makers and their analytic teams in establishing and evaluating their internal standards and procedures for ethical OSINT use. This Scorecard is intended to act as a supplement to the 2022 Public-Private Analytic Exchange Program (AEP) Phase I white paper entitled, "Ethical Frameworks in Open-Source Intelligence".†

INSTRUCTIONS:

Using the rubric to the right, and providing a score of 1-5, determine the degree to which you agree or disagree with the below statements. Add any comments, insights, or follow-up instructions into the notes box.

	Scoring Rubric
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

PRINCIPLE #1: Furthers Mission & Reflects Core Values.

	Activity	Score (1-5)	Notes
☐	Decision-makers are appropriately informed on the types of OSINT activities performed and how they further company goals.		
☐	OSINT analysts are well-versed in the company's value and mission statements and can articulate how their activities align with them.		
☐	Supervisors are present and have an active role in the OSINT analysis and dissemination process.		
☐	The company has a policy of transparency with regards to their OSINT research methodology, as well as their ultimate uses.		
Total			

* ***DISCLAIMER STATEMENT***: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

† Further details on the AEP Program, and a link to the Phase I white paper are provided later in this product.

PRINCIPLE #2: Respectful of Liberty, Civil Rights, and Other Protections.

	Activity	Score (1-5)	Notes
☐	OSINT analysts operate in an environment of restraint, using the "least intrusive means" necessary when performing research on persons.		
☐	OSINT activities are performed in a way that does not infringe on individuals' 1st Amendment‡, 14th Amendment§, or other Constitutional protections.		
☐	OSINT activities are performed in a way that avoids targeting individuals for research based solely on protected status, including race, ethnicity, political beliefs, religion, etc.		
☐	OSINT analysts' findings are presented to customers in a way that separates allegations of crime from determinations of guilt (i.e., respects due process).		
☐	OSINT policies provide guidance to analysts on how to separate professional OSINT activities from analysts' personal rights to access media or engage in other activities outside of work.		
Total			

PRINCIPLE #3: Accurate, Timely, & Customer-Oriented Analysis.

	Activity	Score (1-5)	Notes
☐	OSINT analysts corroborate research with information from other credible sources.		
☐	OSINT analysts can clearly articulate who the primary customer(s) of their research are.		
☐	OSINT analysts, and decision-makers, are both sensitized to one another's info-needs, capabilities, and limitations.		
☐	OSINT analysts have a vehicle that allows them to obtain customer feedback, and they take follow-on actions as needed.		
Total			

‡ The First Amendment prohibits any law limiting freedom with respect to religion, expression, press, peaceful assembly, or the right of citizens to petition the government.

§ The Fourteenth Amendment granted citizenship to all individuals living in the United States.

PRINCIPLE #4: Retention & Audit SOP.

	Activity	Score (1-5)	Notes
☐	OSINT research is always predicated on protecting the company, and its activities, from criminal, violent, or otherwise harmful acts.		
☐	OSINT analysts are trained on of which types of activities, or subjects of inquiry, company deems "out of bounds".		
☐	The company's OSINT activities comply with all federal, state, and local laws.		
☐	Decision-makers considered ways in which the companies' OSINT research could be exploited by other nefarious actors for unintended purposes.		
Total			

PRINCIPLE #5: Empathy & Respect in All Actions.

	Activity	Score (1-5)	Notes
☐	OSINT analysts have a standardized, and easily reviewable, system for cataloguing their research efforts.		
☐	The company has a policy for how, and when, to purge OSINT records after they've lost their utility.		
☐	Decision-makers have considered the legal and reputational implications associated with a hacking, or a data-spill, incident involving OSINT records.		
☐	Decision-makers have identified external, non-affiliated, entities within the company that can perform OSINT record audits.		
Total			
Overall Score			

UNDERSTANDING YOUR SCORE:

After rating your company 1-5 in all activities, tally your score for each principle by adding the scores in the "Total" columns. Then add all 4 of these totals together to determine your Overall Score.

Overall scores can range from 20-100. The below ranges can help to provide suggestions for your companies:

- A score ranging from 20-50 suggests your company may want to consider making changes to strengthen your OSINT policies.
- A score of 50-80 suggests your company likely already adheres to ethical OSINT policies; however, it may be worth reviewing them to with your workforce to ensure broad adherence.
- A score from 80-100 suggests your company likely excels at adhering to ethical OSINT policies.

THE AEP PROGRAM:

The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security on behalf of the US Intelligence Community, facilitates collaborative partnerships between members of the private sector and U.S government analysts to create joint analytic products that address problems of interest to both the private sector and the U.S. Government. See the following link: https://www.dhs.gov/publication/aep-overview-and-documents

Member	Organization
Brittany Krilov	National Insurance Crime Bureau (NICB)
Ryan Gough	Secure Community Network
Patricia Kickland	Hawaii State Fusion Center
Danielle Fiumefreddo Waters	Bank of America
Lauren Szolomayer	Delaware Valley Intelligence Center (DVIC)
Conley H. (Champion)	DHS (Champion Agency)

ASSOCIATED CONCEPTS:

Below is a brief description of some key concepts associated with the topic of OSINT and the establishment of ethical frameworks. A more in-depth examination of many of these matters are found in the 2022 AEP *Phase I* white paper.

Ethical Interpretations. Ethics are, broadly, a set of moral principles and values.[1] Entities in the government and private sector who seek to perform OSINT research, and particularly those using social media, in a principled manner face several challenges, including varying ethical interpretations over time and geography, a lack of generally accepted national or international norms for OSINT use, and evolving concerns because of rapid advances in technology.[2,3]

OSINT Definition. Government practitioners and their academic counterparts have not reached a consensus regarding a definition for OSINT; however, OSINT is generally assumed to concern the gathering of information from publicly available sources.[4,5] The emergence of social media platforms, and disagreements over whether they have associated expectations of privacy, only complicate the definitional debate.[6]

Sensitive Data Access. Some corporate OSINT practitioners, such as those working in the financial, legal, or medical industries, have regular access to particularly sensitive information about members of the public, such as banking and tax information, private legal deliberations, or personal medical histories. Corporate decisionmakers n these industries have a societal duty to establish and uphold ethical guidelines within their companies to protect sensitive information from exposure.

"The Chilling Effect". US Government entities are prohibited from engaging in actions that create a "chilling effect"—deterring individuals from exercising their First Amendment rights, such as free speech or expression.[7] Chilling can also occur at the hands of private parties, acting either illegally or legally.[8] Corporate OSINT researchers, particularly those who share their findings in support of law enforcement investigations, must be aware of their potential chilling effects upon society.

The Fourth Amendment. The US Constitution's Fourth Amendment protects the US public from unreasonable search and seizure.[9] Legal and intellectual experts have long debated what constitutes a

"reasonable" search or seizure, and the emergence of social media and law enforcement's use of OSINT to further their criminal investigations have complicated this debate.[10]

Historical Evolution of OSINT. The first uses of OSINT were primarily in support of US military and foreign policy efforts, such as monitoring and analyzing foreign propaganda in the early years of World War II.[11] In recent years, and increasingly since the emergence of the internet, individuals within nearly all industries use OSINT research to glean publicly available insights in support of their respective mission requirements.

FURTHER INFORMATION:

For corporate entities seeking further information on the topic of ethical OSINT use, see the 2022 AEP *Phase I* white paper entitled, "Ethical Frameworks in Open-Source Intelligence": https://www.dhs.gov/sites/default/files/2022-09/Ethical%20Frameworks%20in%20OSINT%20Final.pdf

Additionally, for entities seeking further research on the topic of ethics and open-source research broadly, we recommend reviewing the United Nation's 2022 online publication entitled, "Berkeley Protocol on Digital Open Source Investigations": https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

Appendix I: The 5 Key Principles of Ethical OSINT

PRINCIPLE #1: Furthers Mission & Reflects Core Values.

Private sector entity analysts and decision-makers who rely on OSINT face ethical challenges regularly, and unfortunately, they have no set of policies with specific guidance to cover every scenario they encounter. However, most private entities have at least one policy that can prove invaluable for ensuring their OSINT activities remain appropriate: Mission and Value statements. Though Mission and Value statements are typically very short in length, they can at a basic level identify what goals the company is seeking to accomplish. Analysts and decision-makers can familiarize themselves with these goals and then determine to what degree their OSINT activities are aligned with them.

For example, a social media company's Mission and Value statement may be to "encourage free expression with few barriers to participation". Based on that foundational statement, one of the company's key goals are to enable information sharing. Therefore, any activity that an OSINT researcher performs that stymies the sharing of information would run afoul of that goal and be contrary to the entity's Mission and Value statement. In other words, if an entity's OSINT activities are not clearly moving the entity toward its stated goals, then Principle #1 suggests that they should avoid engaging in those activities.

Similarly, when private entities establish their intelligence apparatus, decision-makers should have a leadership-approved list of the specific functions that the intelligence office is expected to perform—whether that is informing C-suite executives of how overseas developments may put their employees in harm's way, or whether a particular advertising decision will result in unwanted negative publicity. OSINT researchers should be well-versed in the fundamental roles their job is expected to fill for their parent entity, as this can help them determine what is, and is not, an appropriate use of their tools.

PRINCIPLE #2: Respectful of Liberty, Civil Rights, and Other Protections

The public cares deeply about privacy, civil rights, and civil liberties as they pertain to OSINT. Although private entities do not have the same legal obligations as government entities, the public expects that private entities' activities align with longstanding cultural norms—which stem from the legal protections that limit government entities. Therefore, although private entities may be able to engage in activities that would not be lawful for government entities, private entities are still likely to face criticism about how they use OSINT.

Rather than asking private entities to develop ethical standards based solely on laws that apply to the government, Principle #2 suggests that private entities should apply their own values to consider not only whether the entity **can** engage in OSINT activities, but also whether entities **should** engage in those activities. One suggestion is that entity leadership develop OSINT policies based on constant collaboration and feedback between decision-makers and analysts. Collaboration allows analysts to tailor their activities more narrowly to answer specific questions from decision-makers, thereby minimizing what outsiders may see as analyst overreach. At the same time, through collaboration, decision-makers may become more familiar with analytical tradecraft in a way that lets decision-makers suggest parameters to guide analysts' work.

So, for example, the public may easily understand that private entities have legitimate business interests in conducting marketing research that collects demographic data. At the same time, the public may balk at a revelation that shows a private entity's corporate security department collected data based on protected class status, even if that data collection were not illegal as the law applies to private entities.

Likewise, the marketing department may have a good reason for asking about consumers' opinions on hot button political issues, but a private entity whose Mission and Values statement indicates that it will remain neutral on political issues may have a hard time explaining why its personnel department needed to know about potential employees' political views.

Another consideration is that while an entity's policies may limit OSINT activities during analysts' regular job duties, when the workday is finished and the analysts go home, something may come up in their personal media consumption that would fall outside entity policy. Again, although private entities are not bound by the same legal protections that apply to government entities, it would be difficult to explain what legitimate interest any entity has in a blanket limit on analysts' access to information. Entities may find it beneficial to create policies that are directly tied to job duties rather than applying broad limits to research techniques.

PRINCIPLE #3: Accurate, Timely, & Customer-Oriented Analysis.

OSINT is an extremely broad area of activity, and analysts can perform research and report on OSINT in many ways. Principle #3 ensures that a private entities' OSINT activities are of high quality. A good starting point for analysts engaging OSINT research is to define the purpose of their activities, their customers' needs, and the possible biases all parties may be operating under—specifically, analysts should know exactly what they should research, why they should research it, and how it informs their results.

Additionally, it is worth noting that analysts often face tension between the availability of information and the accuracy of information, i.e., the difference between obtaining the information quickly versus obtaining the correct information. OSINT information tends to be easily obtainable; however, the information may not always be correct if relying on an unreliable or uninformed source. Analysts should take the time to verify that the source from which they are gleaning their information produces high-quality results.

Further, OSINT analysts should be constantly checking their research to ensure its' relevance to their case, while practicing restraint the type and amount of data collected. Analysts may have access to large amounts of information, however, much of it may not have any connection to their initial research topic, so they need to sift the "wheat from the chaff". Analysts are experts at understanding the information contained within their datasets, and as such, they should be aware that the accuracy and utility of the OSINT product they produce is their responsibility.

PRINCIPLE #4: Retention & Audit SOP.

Creating policies that are designed to allow future audits are a must for OSINT researchers. OSINT analysts, for example, may be engaging in OSINT activities that are intended to further a law enforcement investigation, for use in litigation, or in support of human resources (HR) actions against employees. As such, OSINT researchers much be able to explicitly show how they found this information or risk putting the success of these activities at risk. Principle #4 suggests that OSINT managers establish a Standard Operating Procedure (SOP) to ensure uniformity of actions among researchers, and to be able to show under courtroom scrutiny how researchers acted within the normal course of their duties when performing OSINT activities.

Retention and audit SOPs can be useful for doing post-mortem analysis of OSINT researchers' activities during a critical event, allowing the team to learn from their successes and mistakes. A retention and audit SOP can also be useful during quarterly and yearly reviews. Retaining information about specific

OSINT activities can help managers determine which OSINT tools or programs truly offer an entity a positive return on investment.

Further, having a retention and audit SOP is necessary when OSINT researchers inevitably are put into situations in which they must disclose information to outside entities, such as other companies or researchers. Having a good SOP can clearly delineate for OSINT team members which information is acceptable for outside sharing, such as strategic trend information, and which is not, such as personal data.

PRINCIPLE #5: Empathy & Respect in All Actions.

As technology continues to advance, the need for empathy and respect in both policy and practice has never been more evident. Empathy allows people to better understand each other's actions and intentions, while respect promotes an equal and more productive society. Principle #5 applies broadly to ethical frameworks in OSINT, because it supports good outcomes within the entity's workplace and good relationships between the entity and the public. Additionally, promoting empathy and respect within the workplace can advance team moral and cohesion amongst personnel, leading to increased productivity and customer satisfaction.

When dealing with the public, empathy and respect inherently promote transparency and careful thought into how the entity's OSINT activities may be interpreted or perceived. An empathetic and respectful approach to collection, retention, analysis, and dissemination is more likely to receive a positive public response. On the other hand, actions that may be considered intrusive or unnecessary may be the subject of public scrutiny and legal disputes.

In conclusion, OSINT activities grounded in empathy and respect would usually be accomplished through the least intrusive means possible. Analysts acting in good faith should be able to provide a clear and concise reason for each inquiry and justify specific reasoning. OSINT collection should aim to improve operational productivity; however, entities should remain mindful of their mission, values, and intelligence goals, and limit their OSINT activities accordingly.

2023 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Appendix II: Interview Themes

Our AEP research team performed multiple interviews with corporate partners who utilize OSINT research in support of their corporate security activities. During these interviews, the AEP research team asked them basic questions regarding their position within the company, the ways they OSINT research is used to support their business needs, and we asked for their insights on the value of the 5 Principles of Ethical OSINT described in the Scorecard. Below are some of the broader themes we gleaned concerning ethical use of OSINT research from these interviews.

The Court of Public Opinion.

One theme noted by corporate partners was that, though there is little in the way of industry standards and oversight for OSINT use, researchers are still expected to answer to the court of public opinion.[12] For example, corporate intelligence teams can purchase tools from 3rd party vendors that scrape large swaths of public information that likely have some utility in identifying criminal individuals who impact their profits. However, though these companies are not legally prohibited from using such tools, corporate decisionmakers realize that their company would likely face harsh judgment from the public if their use of these tools ever to comes to light, thus they elect to not use them.[13] Further, as one of the most common functions of OSINT research teams is to protect their company's brand from reputational harm, such questionable activities would likely be seen as counterproductive.[14,15]

Restraint.

Relatedly, interviewees indicated that their teams' OSINT research activities occurred in an environment characterized by restraint. OSINT research was performed only when it could be clearly articulated as identifying or mitigating an activity that is a risk to their business, and analysts were prohibited from performing research without a good reason.[16,17,18] Additionally, further restrictions were utilized if OSINT research was focused on individuals, such as during investigative support research—for example, teams took steps to ensure that their activities contained an auditable paper trail, adhered to employment law, and weren't driven by unconscious biases.[19,20]

Mission & Value Statements

Interviewed corporate partners indicated that their Mission and Value statements were somewhat useful in guiding the focus of their OSINT activities, such as in ensuring that analysts can articulate their business case when performing research.[21,22] Some interviewees noted that their Mission and Value statements were unhelpful in directing their OSINT activities due to their vagueness, and apparent inspirational nature rather than providing employees with a guiding principle to operate under. In such cases, companies argued that having an established policy and procedures manual, and an approval hierarchy to determines guidelines is far more valuable.[23]

A Position of Public Trust.

Corporate interviewees, much like law enforcement and emergency management officials, noted that when their teams perform OSINT research they are essentially operating in a position of public trust—and it is up to them to ensure that their activities are appropriate and predicated on furthering a legitimate mission.[24,25] Furthermore, some entities operating in multiple US states noted that some states had more restrictive data privacy laws than others, and that they chose to make their nationwide policies align with the laws of the most restrictive states.[26]

Chain of Custody.

Corporate interviewees stated that in some instances, their duties involved sharing their OSINT research findings with law enforcement. In such cases, they expressed their need for their data to be an audit trail, where they could show research methods with respect to a particular criminal act or individual. Without this, their information may not be admissible in court. [27,28] Other interviewees also noted the need for their company to ensure the safety of their research, and so they ensured their information was kept protected behind a firewall and away from personal email accounts.[29] It is also worth noting that, in some cases, a team's OSINT research efforts were not targeting persons but rather designed to understand the drivers of threats—particularly in those tasked with providing threat assessments for overseas or traveling employees.[30,31]

The Rights of Analysts.

One of the topics that the AEP research team asked corporate interviewees was whether they had concerns that their OSINT policy restrictions might infringe upon the 1st Amendment rights of their own researchers. Interviewees appeared to have been confused by the question.[32,33] Responses included statements indicating that OSINT analysts should not see themselves as facing restrictions due to their operating from a position of public trust.[34] Others were concerned about the possibility that their OSINT researchers might self-censor to the detriment of their mission.[35]

Insider Threat & HR Actions.

Another topic that frequently came up during discussions with corporate interviewees was that their OSINT research was often utilized for the purposes of mitigating threats from within their companies, such as from employees engaging in criminal activity or those that pose a threat of violence in the workplace.[36] Relatedly, interviewees stated the important role OSINT could play in screening applicants for employment, and in the trustworthiness of current employees.[37,38]

---

[1] (U) | Merriam-Webster.com | "Definition: Ethic" | 24 JUL 2024 | Definition of term, "ethic" | https://www.merriam-webster.com/dictionary/ethic | A reliable online publicly available dictionary.
[2] (U) | Velasquez, M., Andre C., Shanks, T., S.J., and Meyer, M.J.; Markkula Center for Applied Ethics | "What is Ethics?" | 1 JAN 2010 | Academic journal article on defining ethics | https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/what-is-ethics/ | A website run by a reputable university.
[3] (U) | Fortin, F., Delle Donne, J., Knop, Justine; Policing in an Age of Reform | "The Use of Social Media in Intelligence and Its Impact on Police Work" | 1 JAN 2021 | Academic journal article on role of social media in policing | https://www.researchgate.net/publication/347408460_The_Use_of_Social_Media_in_Intelligence_and_Its_Impact_on_Police_Work | A chapter in an academic book on modern policing.
[4] (U) | US Code | "Department of Defense Strategy for Open-source Intelligence; Public Law 109-163" | 1 OCT 1996 | Chapter within US Code Title 50 on War and National Defense | https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-subchapI-sec403-5.htm#:~:text=%E2%80%9C(1)%20Open%2Dsource,addressing%20a%20specific%20intelligence%20requirement | A website detailing text from US Code Title 50.
[5] (U) | Rajamäki, J., Sarlio-Siintola, S., Simola, J.; Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS 2018, Oslo, Norway| "Ethics of Open-Source Intelligence

Applied by Maritime Law Enforcement Authorities"; p. 424| 28-29 JUN 2018| Academic journal article examining ethical issues with OSINT in maritime law enforcement| https://www.theseus.fi/bitstream/handle/10024/152174/Rajamaki_Sarlio-Siintola_Simola.pdf;jsessionid=9EE1A1113A8E9E4901E322736B4255EA?sequence=1 | An article in a reputable academic journal.

[6] (U) | Boscolegal.org | "Supreme Court of the United States. U.S. v. Mereglido, 2012 WL 3264501" | 2012 | Website summarizing significant legal cases on social media law | https://www.boscolegal.org/resources/social-media-case-law/#62bf2142ae526 | The website of a reputable legal firm.

[7] (U) | Schauer, F.; William & Mary Law School—Faculty Publications | "Fear, Risk and the First Amendment: Unraveling the Chilling Effect; p. 689" | 1978 | Law journal article on factors impacting 1st Amendment protections | https://scholarship.law.wm.edu/facpubs/879 | An article in a reputable law journal.

[8] (U) | Youn, M.; Vanderbilt Law Review | "The Chilling Effect and the Problem of Private Action; p. 1537" | 2019 | Law journal article on government and corporate actions that harm 1st Amendment protections | https://scholarship.law.vanderbilt.edu/vlr/vol66/iss5/3 | An article in a reputable law journal.

[9] (U) | Constitution of the United States | "Fourth Amendment" | 2023 | Text of the US Constitution's Fourth Amendment | https://constitution.congress.gov/constitution/amendment-4/ | A US government website.

[10] (U) | Judicial Learning Center | "Your 4th Amendment Rights" | 2019 | Analysis of protections afforded to US public by Constitution's Fourth Amendment | https://judiciallearningcenter.org/your-4th-amendment-rights/ | A reputable legal education website.

[11] (U) | Leetaru, K.; CIA Studies in Intelligence | "The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008" | 2010 | History of OSINT activities by US government | https://www.cia.gov/static/e4cd771e0aecd4492cd7e1be1e43fd76/The-Scope-of-FBIS.pdf | A US government industry journal.

[12] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.

[13] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.

[14] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.

[15] (U) | Interview | Research Interview | 13 JUN 2023 | AEP Interview with corporate financial entity | Virtual | An employee of a US finance company.

[16] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.

[17] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.

[18] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.

[19] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.

[20] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.

[21] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.

[22] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.

[23] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.

[24] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.

[25] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.
[26] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.
[27] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.
[28] (U) | Interview | Research Interview | 21 JUL 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.
[29] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.
[30] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.
[31] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.
[32] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.
[33] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.
[34] (U) | Interview | Research Interview | 8 JUN 2023 | AEP Interview with corporate retail entity | Virtual | An employee of a US corporate retail company.
[35] (U) | Interview | Research Interview | 24 MAY 2023 | AEP Interview with sports entertainment entity | Virtual | An employee of a US sports entertainment company.
[36] (U) | Interview | Research Interview | 18 JUL 2023 | AEP Interview with corporate IT entity | Virtual | An employee of a US IT company.
[37] (U) | Interview | Research Interview | 13 JUN 2023 | AEP Interview with corporate financial entity | Virtual | An employee of a US finance company.
[38] (U) | Interview | Research Interview | 13 JUN 2023 | AEP Interview with food service entity | Virtual | An employee of a US food service company.