

ISIR Journal of Arts, Humanities and Social Sciences (ISIRJAHSS)
ISSN: 3048-7463 (Online)
Frequency: Bimonthly
Published By ISIR Publisher
Journal Homepage Link- https://isirpublisher.com/index.php/isirjahss

The Legal and Ethical Implications of Sharing Open-Source Intelligence Among Agencies and Contractors

By

Mike Potter

Mississippi State University William Bonduris



Article History

Received: 12/07/2025
Accepted: 28/08/2025
Published: 24/09/2025

Vol – 2 Issue –5

PP: -08-16

Abstract

This article seeks to understand open-source intelligence in the 21st century by examining the implications of sharing it with high-reliability organizations, private military contractors, and other outside groups. By comparing the efficacy of finished intelligence collected through overt and covert means, we conclude that OSINT can be far more impactful, primarily because it is easily shareable. The article then begins to develop a framework with which to understand the sharing of OSINT and the nature of its potential impacts. Finally, this analysis concludes that OSINT's most useful place auxiliary method to disconfirm traditional intelligence and work as an informational proxy that allows the broad sharing of collected information.

Introduction

Flawed assessments of raw intelligence led to the Second Iraqi War. In part, this occurred because those tasks with finishing intelligence reports failed to share information as broadly as possible (McChrystal 2015). While the special operations community in the military facilitates the movement of information up the chain of command (Broadwel1, 2012: Kaplan, 2013:McRaven, 2019: Petraeus, 2009), the intelligence community was still hampered by the natural hierarchy of the classification of the material (Rosenberg, 2020).

This analysis aims to understand better efficient and effective ways intelligence can be shared, as broadly as possible, in order 1) better vet intelligence without security risk and 2) allow the final intelligence to be as impactful as possible. Underlying this analysis is the idea that intelligence classification acts as a barrier to incorporating the broad range of views and expertise necessary for intelligence to function as well as needed (Bruce and George, 2015). While one may initially assume that sharing open-source information would pose little ethical and legal implications due to it being open-source, this is not the case. There is a crucial difference between open-source information and open-source intelligence. Once open-source information is acted upon by intelligence analysts (raw intelligence), such "finished" information becomes open-source intelligence (OSINT). Therefore, while the basis for the intelligence may have been gathered initially from publicly available information, once that information has been acted upon and turned into intelligence, it is essential to treat it differently and understand where a citizen's privacy may come into play.

Further, when seeking to share intelligence and information, it is essential to identify whom such information will be shared with. In most cases, the American federal government shares its intelligence and information with private military contractors (PMCs), small teams, high-reliability organizations (HROs), and nongovernmental organizations (NGOs). Therefore, it is crucial to clearly define these groups in an academic context and then highlight the ethical and legal dilemmas that may arise when the American federal government shares OSINT with these groups.

Private Military Contractors (PMCs)

Before discussing the legal and ethical implications of sharing OSINT with PMCs, defining what PMCs are is essential. Perhaps the most thorough definition of PMCs is that "PMCs are companies selling services (logistics, consultancies/training or direct armed security provision) in the context of armed conflicts (declared war or not)" (Leander 2010, p.467). Further, Leander also notes that it is often fair to refer to PMCs as "military" and also notes that "these

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

companies are often 'security' companies; the conflicts are often not 'international'; and those who buy the services are usually not public armed forces but NGOs, firms or governmental agencies" (Leander 2010, p. 467). Furthermore, "the companies rarely define themselves as military" (Leander 2010, p. 467). These clarifications are necessary to recognize because they underscore the degree to which PMCs evolve to fit different situations and should not merely be thought of in a traditional warfare setting. Further, it is vital to define PMCs with specificity when discussing the implications of sharing OSINT. If any of these details are ignored, it could allow for a dangerous loophole in the information sharing protocol. However, there are other useful definitions of PMCs to consider, such as the idea that PMCs are "any private contractor or private contracting firm that provides logistic support, consulting services, technical services, or security functions as a substitute for a military force" (Stanley 2015, p.174). It bears mentioning that both Stanley and Leander's definitions of PMCs highlight all PMCs' various roles, including logistics, consulting, or technical services. These roles for PMCs must be included in the discussion of OSINT sharing because it is likely that shared OSINT will be used in a capacity outside traditional warfighting. Understanding the various details that need to be included when discussing PMCs, one then learns how deeply involved in warfare PMCs are. This deep-rooted involvement leads to multiple concerns about sharing OSINT information with these groups.

With a grasp of how PMCs are defined in academic texts, one can then examine the key issue when discussing the federal government's sharing information with PMCs. The fundamental problem of sharing OSINT with PMCs is the fact that "private contractors are not State officials, which renders it very difficult to prosecute and punish their acts, especially when committed on foreign soil, and not surprisingly the record of criminal prosecutions concerning acts committed by PMSCs' employees is remarkably low" (Frulli 2010, p. 436). This is a crucial point because if the U.S. government were to act in ways that violate American citizens' rights, those citizens have ways of conducting oversight and instituting policy changes through their elected representatives and civilian leadership of the military. However, civilian oversight is much more difficult to conduct on private businesses. Thus, if the U.S. government collects open-source information about American citizens and acts upon it, turning it into OSINT, it may be one matter entirely for the government to act upon that or share that information internally, but completely different to share that with outside private organizations. This difference stems from the fact that the military must adhere to certain transparency levels while PMCs can operate in an opaquer fashion. A potential solution to this problem would be for the military to insist on specific best practices and conduct some degree of oversight over PMCs, but that could put the military in a position it has not traditionally held. Even some oversight and contract stipulations on PMCs would likely not eliminate PMCs' chance of violating citizens' rights or abusing OSINT. Further, this is only contending with the issues that might arise legally for domestic PMCs to use OSINT about American citizens or domestic actors as it could likely become an even more complicated situation if the American military were sharing information with foreign PMCs about American citizens or contracting with foreign PMCs to then conduct operations against citizens of that PMC's country or another third country. Overall, involving PMCs in handling potentially sensitive information about American citizens or others could open a Pandora's Box of legal and ethical dilemmas due to the lack of civilian oversight and transparency.

Ultimately, with an understanding of how PMCs are defined and the vast array of functions they can perform for the federal government, it becomes apparent how closely the federal government is intertwined with PMCs when it comes to military defense. This close connection means that it is very likely that the federal government will be willing to share OSINT with PMCs to help achieve their desired military outcomes. However, despite the broad ethical and legal implications of sharing OSINT that will be discussed further, the federal government sharing OSINT with PMCs may not be advisable unless stringent privacy protections and oversight could be ensured. This is because the federal government must be accountable to the American people and their representatives, which currently occurs through congressional oversight and hearings. However, private companies like PMCs have no duty to submit to oversight. Thus, if they were to misuse OSINT or violate American citizens' privacy in any way, it would be much more difficult for the federal government to extract recourse from a PMC than it would be to discipline public defense agencies.

Small Teams and High-Reliability Organizations (HROs)

The second type of groups that are important to include in the discussion of OSINT sharing are small teams and HROs; it is also essential to define what these groups understand the ethical and legal implications of sharing information. HROs are primarily discussed as being outside the military and are broadly defined as "an organization that has succeeded in avoiding catastrophes despite a high level of risk and complexity" (Jacobson, 2019). This can also be understood to inhibit situations that are potentially fraught with accidents, yet they operate nearly error-free (Christianson et al. 2011, p.2). Some HROs include nuclear powerplants, aircraft carriers, and air traffic controllers (Jacobson, 2019). Further, while small teams are a less formal category than HROs, remote teams can be understood as "larger than three but not more than eight members" (Adams & Webb 2002). With examples including "armored vehicle crews, infantry assault groups, artillery teams, crews of larger aircraft, surveillance teams, sensor or warfare teams on warships" (Adams & Webb 2002). Further, it is essential to note that "while larger military groups such as army platoon and company size groups and above are beyond the present scope, temporary teams such as command or planning teams of four or five people fall within the working definition of a small team" (Adams & Webb 2002). These distinctions are important to note because HROs and small teams inherently make different cases for having OSINT shared with them. Thus, it is crucial to further delve

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

into the issues that may arise in sharing OSINT with HROs and small teams.

With an understanding of the definition of HROs and small teams, it is essential to then examine potential issues with the federal government sharing OSINT with these organizations. One potential problem with the federal government sharing information with HROs is who determines their high-reliability status. This could become an issue because HROs would likely exist outside of the federal government in the form of private contractors. Thus, the government would be imparting a high degree of confidence and privilege in these outside groups that may be misplaced. Therefore, it would be imperative for the federal government to develop a uniform, standardized process for determining what an HRO is or how that status is determined. A method for granting such status could ensure that certain precautions are taken by the HRO and ensure potential liabilities are clarified in case of a failure on the part of the HRO in using OSINT. Despite the implications of sharing OSINT with HROs, it seems as though small teams would be ideal for OSINT sharing. In the previously mentioned definition, the small groups would be teams within the American military and would not exist outside of civilian oversight. However, despite the benefits of oversight, there would still be concerns about ensuring small teams could properly use OSINT. Nevertheless, such problems exist outside of the discussed legal and ethical implications. However, it becomes vital to delve into HROs because they are a formal category outside of the military, unlike small teams.

In suggesting that the federal government certify outside HROs, it becomes relevant to understand further what characteristics make an HRO. Therefore, it is essential to note that some attributes of an HRO that have been identified are a preoccupation with failure, a reluctance to simplify, sensitivity to operations, a commitment to resilience, and deference to expertise (Jacobson, 2019). In general, HROs differentiate themselves from other organizations by not sweeping failures under the rug (Jacobson, 2019). Instead, they zero in on them because, in aircraft carriers or nuclear power plants, a minor mistake could lead to massive danger for those directly involved and others outside the situation. This same type of preoccupation with failure would need to be paid to OSINT to prevent data breaches and vigilantly ensure that rights are not violated.

Further, HROs embrace their complexity by rejecting simple explanations for failure or difficulty (Jacobson, 2019) and are willing to shift their core beliefs when data indicates that it should. This would be crucial in dealing with OSINT because it would ensure that HROs recognize the value of protecting OSINT and allow OSINT to identify alternative explanations or solutions to problems potentially. HROs are also sensitive to operations and thus place a high value on front-line operators' opinions (Jacobson, 2019). This value could be crucial in preventing data breaches of OSINT and ensuring that the work of OSINT analysts is valued and examined. Further, HROs' commitment to resilience ensures that they will seek to anticipate difficulties and adapt to fix the situation rather than merely bandage over the problem. Finally, HRO's deference to expertise provides that they carefully examine OSINT to glean as much useful information as possible rather than emphasize information that merely supports an already crafted narrative. While HROs certainly embody many desirable characteristics, there are still legitimate concerns with the federal government sharing OSINT with them.

However, with an understanding of the definition and characteristics of HROs, it is also essential to recognize their limitations. For example, Christianson makes the point that "high reliability is not a state that an organization can ever fully achieve; rather, it is something the organization seeks or continually aspires to" (Christianson et al. 2011, p.2). Further, "reliability is fundamentally a dynamic set of properties, activities, and responses" (Christianson 2011 et al., p.2). These ideas highlight the fact that despite their impressive success, HROs still face many risks. Therefore, if OSINT is shared with HROs without substantive oversight and procedures, then the daily threat that HROs face could, in turn, be posed to OSINT as well. While there are specific concerns about the legal and ethical implications of sharing OSINT with HROs, it is essential to note that many of these concerns are not as relevant because small teams exist within the military. This highlights the importance of the military using in-house groups rather than outsourcing. Many of the legal and ethical implications of sharing information come from an organization's status outside the government and thus separate from oversight.

Nongovernmental Organizations (NGOs)

NGOs are the third type of group that is important to include in the discussion of OSINT sharing. Thus it is also vital to define NGOs to illustrate the ethical and legal implications of sharing information. The current United Nations (UN) requirements for NGOs are that they must have "an established headquarters, an executive organ, and officer, a democratically adopted constitution (providing for the determination of policy by a representative body), an authority to speak for the members, and financial independence from governmental bodies" (Martens 2002, p.74). Further, in continuing with the UN perspective on NGOs it "now interprets the term NGO as referring to national, regional, as well as international actors, the initial interpretation of NGOs as "international" organizations may today be seen as anachronistic" (Martens 2002, p.282). Furthermore, another essential aspect of NGOs is that they are "formal (professionalized) independent societal organizations whose primary aim is to promote common goals at the national or the international level" (Martens 2002, p.282). This is crucial to understand, as it highlights that NGOs must be professional and promote common goals. However, while international security is undoubtedly a common goal that could justify information sharing from the American government to NGOs, there is still more to consider in sharing OSINT with NGOs.

While the UN definition of NGOs is essential to consider, it is also relevant to recognize other NGOs' definitions.

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Specifically, sociological approaches to defining NGOs have been vaguer than the UN position. For instance, some definitions define NGOs as "nongovernmental, non-profit-making, not-uninational" (Martens 2002, p.278), while others include specific details and define NGOs as "any non-profit-making, non-violent, organized group of people who are not seeking governmental office" (Martens 2002, p.278). Specifically, noting that an NGO is non-violent is a crucial piece of defining NGOs. A vague definition lacking nonviolence as an attribute could potentially include terrorist or criminal organizations such as the Irish Republican Army and the mafia as NGOs (Martens 2002, p.279). Crucially, as the name indicates, "governments or governmental components are excluded from the definition of NGOs" (Martens 2002, p.280).

Further, "NGOs are generally understood as being organizations that do not include governmental representatives" (Martens 2002, p.280) and that they "are made up of individuals or national groups (which contain only individuals) and not official representatives of national governments" (Martens 2002, p.280). Another crucial element of NGOs is that they "must not be dependent significantly on governments for financial and moral support (Rosenau, 1998)" (Martens 2002, p.280-281). However, it is essential to note that NGOs "may receive financial contributions from governmental sources, but only to a limited extent so that they are capable of maintaining themselves in case governmental contributions are withdrawn" (Martens 2002, p.280-281). Despite this stipulation, many NGOs make government contracts a large part of their operations, and thus their financial success is directly tied to a foreign government. Therefore, this idea of NGOs not being dependent on a foreign government has holes in it (Martens 2002, p.280-281). However, NGOs' overall lack of government presence is crucial to understanding the concerns with the American government sharing OSINT with NGOs. This is because NGOs must, by definition, have limited government control. Thus if the American government were to share OSINT with an NGO, it would likely want to exert control over how and what an NGO can do with that OSINT, which could functionally change that organization's NGO status as it would be following the orders of a national government. Further, sharing OSINT with NGOs could be risky, as it may distract from NGOs' often-charitable missions. Thus, if the federal government were to enlist the help of an NGO by sharing OSINT information, it could jeopardize that NGO's mission abroad and perhaps make an international situation worse.

Ultimately, a key theme that reoccurs with each of the three organizations that could have OSINT shared with them is that merely because it is open-sourced does not negate the fact that it is still intelligence. Thus, it should be treated with all the care and secrecy that any other kind of intelligence would be treated with. Further, sharing information about American citizens without their knowledge or consent with groups outside the federal government represents a significant ethical concern in dealing with citizens' privacy. Overall, these ethical and legal concerns apply to NGOs. Not only could it interfere with an NGO's mission and status, but it could also violate American citizens' privacy.

Current Information Sharing Environment

When examining the legal and ethical implications of sharing OSID with outside groups, it is essential to understand what the current information sharing environment is within the government and outside the government. Currently, the federal government is experiencing a marked improvement in information sharing within the Intelligence Community (IC) as it has begun to move towards "a model in which data sharing is encouraged, not disfavored" (Goldstein, 2017). Further, "about five years ago, the IC moved away from siloed IT and established the IC Information Technology Enterprise" (Goldstein, 2017), which "is a platform of nine shared services, including security, networking, email, and virtual desktops, all delivered via a private cloud" (Goldstein, 2017). This represented a significant change in the IC because the IC viewed information sharing as a weakness for many years. After all, not only could it represent an avenue for information to be intercepted, but it could also allow other intelligence or military groups to get involved and potentially disrupt one agency's plans. However, it seems as though the IC has begun to come around to the idea that sharing information rather than hoarding can allow for more effective fulfillment of mission objectives (Tynan, 2017). Thus, this has been a critical development for the 17 agencies that make up the IC (Tynan, 2017).

Further, former Acting Chief Information Officer (CIO) of the IC, Jennifer Kron, has noted that within recent years "the IC has been using technology to break down barriers between agencies and to make intelligence data a community asset" (Tynan, 2017). Kron also contends that the critical barrier that remains to information sharing within the IC and the federal government is cultural rather than technological. Many agencies are still protective of their data or concerned that policy or security discourages data-sharing (Tynan, 2017). Another piece of information sharing context within the federal government is that 47,000 emergency managers, law enforcement officers, intelligence analysts, and other public safety officials rely on the Homeland Security Information Network (HSIN) to support critical information sharing (ISE, 2016, p.4). Thus, this indicates that information sharing has become imperative in the federal government as it is being used to deal with incidents domestically and incidents that involve other countries. However, it is also relevant to recognize the prevalence of information sharing outside the federal government. For example, "Corporations such as Goldman Sachs use publicly sourced market and political intelligence to identify risks, while international NGOs protect their supply chains using intelligence about terrorist groups gathered from social media and messaging apps" (Hu, 2016). Further, "think tanks such as the Institute for the Study of War, which solely uses OSINT, report on incidents and shifts in armed groups' allegiances at a level of detail that would give intelligence agencies a run for their money" (Hu 2016). This is important because it indicates that, like the IC, groups outside the federal government already share

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

information and are eager to continue. This has potential ramifications for sharing OSINT with outside groups because it shows that outside groups may know how to share and utilize OSINT securely. However, it could also make it difficult for the federal government to resist sharing OSINT, thus underscoring the importance of developing robust OSINT sharing protocols.

Ethical Implications

With an understanding of the definitions of PMCs, HROs, small teams, and NGOs, as well as the broad concerns about information sharing and the information sharing environment, one can begin to look at the ethical implications of OSINT sharing specifically. While some may downplay the value of ethical concerns in favor of merely focusing on the bare minimum of legal compliance, it is essential to note that "legal compliance is just one part of a much bigger picture, and it often forms the lowest bar rather than the best practice we should strive for" (Hu 2016). It is essential that a government and a defense apparatus that is answerable to the people of the United States strive to do more than the bare minimum of legal compliance and instead stand as an ethical model to the world due to the global scale of the American military. This idea is crystallized in the ethical maxim that "the fact that we are not ***prohibited*** from doing something does not mean that we ***should*** commit that act" (Hu 2016). This is a crucial idea for the federal government to observe when considering sharing OSINT because OSINT is an area without much legal guidance on what can be shared or not. Thus, having few set in stone limitations may tempt some to act in ways that could violate privacy and trample over ethical concerns.

Further, before understanding how the federal government should approach ethical issues, it is vital to recognize the ethical issues with sharing OSINT. For example, ethical issues could include "disproportionate interference with the privacy of innocent individuals or groups, risk of outright discrimination, unfair access of some vulnerable or disadvantaged groups to criminal justice of public security, Police officers rights to a private life and freedom of expression" (Rajamäki et al., 2018, p.428). It is essential to understand that while some may dismiss these ethical concerns due to their emphasis on domestic use of OSINT if the federal government shares OSINT without proper precautions, it could very well lead to OSINT being used against domestic populations. Thus, possibly having adverse effects on average citizens, law enforcement, or even intelligence analysts themselves. With just a cursory glance at the potential consequences of OSINT sharing, it becomes apparent that the ethical implications of OSINT sharing are wide-ranging. This is why Eijkman and Weggemans highlight the fact that "from a human rights perspective, the gathering of OSINT demands proper checks and balances" (Eijkman & Weggemans 2012, p.286) and that "this is especially important when security — and intelligence agencies, as well as private companies, use, and exchange information" (Eijkman & Weggemans 2012, p.286). This shows that ethics professionals have recognized the risks associated not only with OSINT but specifically sharing OSINT with outside groups.

Despite the well-illustrated risks of sharing OSINT, it is also crucial that ethical guidelines are not merely implied but laid out to be followed. Thus, some OSINT practitioners have identified strategies to ensure ethical OSINT sharing. These strategies include considering the origin and intent of sources, understanding that while something may be unclassified, it could still be sensitive, understanding that the mosaic effect can allow for anonymized data to be rebuilt and made identifiable, to be wary of reliance on automated analysis, and recognize publicity and visibility (Hu 2016). While these may sound like simple things to be aware of, the federal government needs to identify and disseminate these ethical tips so that OSINT analysts and collectors recognize that open source does not mean immune from risk. However, some groups go further than just recommending ethical ideas to keep in mind. For example, the Stanley Center suggests an organization involved in the use of OSINT develop decision-making frameworks, codes of conduct, and discourse and moral reasoning to determine what the ethical lines in OSINT are (Loehrke et al., 2020, p. 3-5).

Further, explicitly concerning decision-making frameworks, they suggest they use the Markkula framework, a ten-step process that includes sections that focus on recognizing an ethical issue, getting the facts, evaluating alternative actions, making a decision and testing it, and acting and reflecting on the outcome (Loehrke et al., 2020, p. 4). While this may seem like an intensive process, ensuring that OSINT is collected and shared ethically is crucial. However, others suggest going further than merely implementing ethical guidelines instead of fundamentally designing OSINT in an ethical way. An example of this would be to use the privacy by-design approach, which is "an approach to systems engineering intended to ensure privacy protection from the earliest stages of a project and to be taken into account throughout the whole engineering process, not just in hindsight" (Rajamäki & Simola, 2019, p. 365). The framework for privacy by design is understood as having eight significant components, minimize, hide, abstract, separate, inform, control, enforce, and demonstrate (Rajamäki & Simola, 2019, p. 365). Each of these components is intended to make OSINT more protective of individuals' privacy by obscuring many details about the information collected and empowering citizens to understand how their data could be used as OSINT. Overall, each of the various strategies for avoiding ethical quandaries highlights the need for OSINT practitioners to be keenly aware of the ethics of what they are doing and recognize when they may be crossing a line. Further, the ethical risks associated merely with collecting OSINT highlight the cascading ethical implications that could occur when sharing OSINT with outside organizations that cannot ensure the same ethical standards.

Understanding some strategies for making OSINT more ethical is also essential to discuss why the simple legal compliance standard is insufficient. One issue that complicates OSINT and allows for many of the ethical

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

dilemmas surrounding open-source intelligence is the lack of clarity around the difference between OSINT and open-source information and what kind of ethics is used to view the practice (Bean, 2011, p.386). Therefore, in addition to developing ethical guidelines for OSINT, it is also incumbent upon the federal government to utilize uniform, ethical definitions that meet a standard of legal compliance and go beyond that. Further, it is also important to note that "even though laws, regulations, and policies concerning OSINF may recognize the need for checks and balances including the value of the right to privacy, data protection or a fair trial, it is nevertheless important to review whether the gathering of OSINF online requires more (state) accountability" (Eijkman & Weggemans 2012, p.286). This is crucial for the federal government and OSINT practitioners to understand because it highlights the importance of ethical considerations beyond mere legal compliance. Overall, while there must indeed be a minimum standard that the federal government enacts when considering sharing OSINT, there must also be clear ethical guidelines that must be met.

Finally, the federal government must recognize that sifting through the ethical dilemma is not incumbent on the intelligence analyst or practitioner because their actions would be prescribed by law and policy. Instead, the ethical dilemma would be on the government for upholding the law or policy with ethical dilemmas (Bean 2011, p.386). Therefore, the federal government cannot merely pass the buck and expect outside groups to follow a higher ethical standard than legal compliance. Furthermore, it is also worth noting that "it is questionable whether all responsibility for a proper functioning and use of OSINT platforms can be ascribed to the end-users; and some responsibility for a proper functioning of OSINT framework in practice also lies with the developers of the platform and individual components" (Rajamäki & Simola 2019, p. 366). This is vital because while it does put an onus on open-source developers, it does not absolve the federal government of ethical responsibility. After all, the federal government will likely be a large consumer of OSINT platforms. Thus, through close work with the platform vendors, the federal government has a responsibility to insist that OSINT platforms be made ethically. Overall, suppose the federal government wishes to collect and share OSINT. In that case, it must clearly define OSINT and lay out both the legal compliance and ethical standards that must be maintained and threaten severe recourse if any of these rules are violated. Sharing OSINT is a fraught route with risk and filled with a potential reward so long as it is done ethically.

Legal Implications

With a grasp on the ethical implications of sharing OSINT, it is also essential to explore the legal consequences of sharing OSINT with outside groups. Thus, it is vital to understand what laws currently govern information sharing and the legal implications of information sharing. While information sharing in the IC has not traditionally been a high priority, it has become more vital in recent years (Goldstein, 2017). Thus, as information sharing across intelligence agencies has become more popular and encouraged, it is unsurprising that questions about sharing OSINT would arise. As discussed, the most likely targets for sharing OSINT would be PMCs, HROs, small teams, and NGOs. Therefore, it is essential to delve into any relevant statutes and potential legal implications of sharing OSINT with outside groups.

While there is a litany of laws surrounding the United States' defense apparatus, there is very little written about sharing information and specifically sharing OSINT with outside groups. Therefore, one must look to general information sharing laws within the defense apparatus to understand where legal complications may arise. Perhaps the defining law of sharing information in recent years has been the Cybersecurity Information Sharing Act of 2015 (CISA). This Statute "was established to improve cybersecurity in the United States through enhanced sharing of cyber threat information" (Office of the Inspector General of the Intelligence Community [OIGIC] 2019, p.1). Further, the critical piece of this law is that "the Statute creates a framework to facilitate and promote the voluntary sharing of cyber threat indicators and defensive measures among and between Federal and non-Federal entities" (OIGIC 2019, p.1). What makes this Statute so relevant to OSINT sharing is the idea of voluntary sharing with non-Federal entities. This is because the OSINT sharing that has been discussed would certainly be voluntary and specifically hinges on sharing with non-Federal entities like PMCs, NGOs, and HROs.

Furthermore, "Cybersecurity threat" is broadly defined to include action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system" (OIGIC 2019, p.1). This legislation is also important to highlight because a narrower understanding of cybersecurity may not include OSINT, but because CISA broadly defines cybersecurity, it could consist of OSINT. Thus, under this current definition, cyber threat indicators could come from OSINT, which means that in sharing these indicators, the federal government would be sharing OSINT. Due to the lack of more specific legislation, this Statute provides the basis for the legal implications of OSINT sharing. That basis makes a strong case that OSINT sharing with outside groups is not only allowed but is currently happening.

While this legislation is significant for merely creating a system to share information between government and outside groups, it also touches on some potential ethical complications and offers a policy to avoid them. Thus, it is essential to discuss the fact that "other key provisions in the legislation include protection from liability for private entities that share cybersecurity information following established procedures, and the protection of privacy and civil liberties when implementing the Statute" (OIGIC 2019, p.4). Further, "the Statute calls for the removal of information not directly related to a cybersecurity threat that is known at the time of sharing to be the personal information of a specific individual or information that identifies a specific individual" (OIGIC 2019, p.4). These are essential pieces of legislation to highlight because they protect outside groups who share

*Corresponding Author: **Mike Potter**

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

information appropriately and outline critical privacy protections that should be taken when sharing information. These provisions are vital because protecting outside groups who share information appropriately can be an excellent tool to ensure appropriate sharing procedures. Further, it is noteworthy that the CISA legislation was keen to enshrine privacy protections for citizens through anonymizing data. These other legislation sections are crucial to recognize because they deal with potential ethical issues in data sharing.

With an understanding of the legislation which currently minimizes the legal implications of OSINT sharing, it is crucial to further delve into what information sharing is already being conducted under this Statute and examine how it compares to potential OSINT sharing. First, "the OIGs determined that sharing of cyber threat indicators and defensive measures has improved over the past two years and efforts are underway to expand access to information" (OIGIC 2019, p.1). Thus, it is apparent that information sharing has ramped up under this Statute. Further, "sharing cyber threat indicators and defensive measures increases the amount of information available for defending systems and networks against cyber-attacks" (OIGIC 2019, p.1). This piece is important because it highlights the idea that more information is the key to preventing cyber-attacks. Thus, more information could strongly justify sharing OSINT with outside groups. However, it is essential to point out that "using the Automated Indicator Sharing (AIS) remains a challenge. Specifically, the number of nongovernmental entities using AIS is minimal, and other challenges with AIS information deter its use." (OIGIC 2019, p. 2). This clearly states that while minimal, nongovernmental entities currently share information through AIS. Therefore, if nongovernmental entities are already engaged in sharing information, that could be argued is OSINT due to the broad definition of "cybersecurity threat." The federal government is already sharing OSINT with outside groups. Thus, the legal implications of sharing OSINT would be null because they would already be authorized and taking place under CISA.

While it may be alarming to some that sharing OSINT with outside groups could currently be happening, some information that may assuage ethical concerns is the fact that the Inspector General of the Intelligence Community's report states that in recent information sharing, the government "did not receive information that was unrelated to a cybersecurity threat that included personal information of a specific individual or information identifying a specific individual" (OIGIC 2019, p.2). This is important because it may show that the government and outside groups can ethically share information, making a strong case that they can continue to do so with express permission to share OSINT. The report goes on to say that the government "did not receive notices due to a failure to remove the information not directly related to a cybersecurity threat that was the personal information of a specific individual" (OIGIC 2019, p.2), nor did the government "need to take steps to minimize adverse effects on the privacy and civil liberties of United States persons from activities carried out under the Statute because there were no known adverse effects" (OIGIC 2019, p.2). Overall, this report suggests that the information sharing that is currently happening is being done ethically and could serve to assuage concerns that OSINT would be shared in risky or unethical ways if it was allowed to be shared with outside groups.

Overall, while there are many legitimate, ethical concerns over information sharing and specifically OSINT sharing with outside groups, it seems as though the legal implications may be null due to CISA. This is because CISA already allows information sharing between federal and non-federal entities, and information sharing has been dramatically encouraged in the IC in recent years. Further, because CISA broadly defines "cybersecurity threat," one could argue that certain OSINT would need to be shared to defend against cybersecurity threats. Thus, OSINT could currently be transferred to non-federal entities under CISA. Therefore, if CISA presently legalizes some form of sharing OSINT with outside groups, there would be minimal legal implications for sharing OSINT. Primarily if OSINT was transmitted using the same ethical practices that are already being used under CISA. Therefore, the only legal hurdle would likely be to have specific legislation or regulations enacted that allowed for sharing OSINT with outside groups. Ultimately, there are still ethical concerns to contend with in OSINT sharing. Always, legally it seems as though a strong argument could be made that OSINT sharing could currently happen and is being done ethically.

Conclusion

In conclusion, with a broad understanding and overview of PMCs, HROs, small teams, and NGOs, it becomes apparent that information sharing with these various groups could be useful. However, it also highlights essential concerns over privacy, discrimination, accountability, and oversight. These concerns are only further encouraged by the present information-sharing environment in which information sharing in the IC has increased rapidly. However, despite significant ethical concerns, there appears to be no major legal concerns with OSINT sharing to outside groups due to CISA. This is because CISA enables information sharing between federal and non-federal groups as well as nongovernmental groups.

Further, CISA broadly defines "cybersecurity threats," which allows one to argue that OSINT should be shared to prevent cybersecurity breaches. Therefore, it could be argued that legally OSINT sharing with outside groups could happen under CISA. However, while this may alarm those with ethical concerns, it is essential to note that any potential sharing has resulted in no ethical complaints or missteps and thus indicates that future sharing could follow the same path. Ultimately, there are always risks associated with sharing citizens' information with outside groups because citizens can oversee their government and hold them accountable. In contrast, they have little power over nongovernmental or private groups. Therefore, OSINT sharing with outside groups will likely occur despite the privacy risks if it is not already happening. While this may be a useful new tool, it is crucial that the federal government heeds the advice of ethicists and

*Corresponding Author: **Mike Potter**
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

develop codes of conduct or guidelines for sharing OSINT and enforces them as they have been doing. Overall, so long as privacy and civil liberty concerns are safeguarded, the powerful tool of OSINT will likely grow in prominence within the United States' defense apparatus.

References

1. Adams, Barbara, and Robert Webb. "Trust in Small Military Teams." 2002.
2. Bean, H. (2011), "Is open source intelligence an ethical issue?", Maret, S. (Ed.) *Government Secrecy* (*Research in Social Problems and Public Policy*, *Vol. 19*), pp. 385-402.
3. file:///C:/Users/William/Downloads/Is_open_source_intelligence_an_ethical_i.pdf
4. Broadwell, P., & Loeb, V. (2012). *All in: The education of General David Petraeus*. New York, NY: The Penguin Press.
5. Christianson, M. K., Sutcliffe, K. M., Miller, M. A., & Iwashyna, T. J. (2011). Becoming a high reliability organization. *Critical Care*, *15*(6), 1-5.
6. Department of Homeland Security. (2016, March 16). DHS/CISA/PIA-029 Automated Indicator Sharing. Retrieved fromhttps://www.dhs.gov/publication/dhsnppdpia-029-automated-indicator-sharing
7. Bruce, J. B., & George, R. (2015). Professionalizing Intelligence Analysis. *Journal of Strategic Security*, *8*(3), 1–23. Retrieved from JSTOR.
8. Frulli, M. (2010). Exploring the Applicability of Command Responsibility to Private Military Contractors. *Journal of Conflict and Security Law*, *15*(3), 435-466.
9. Goldstein, P. (2017, August 21). The Intelligence Community's Top 3 Cybersecurity Priorities. Retrieved from https://fedtechmagazine.com/article/2017/08/intelligence-communitys-top-3-cybersecurity-priorities
10. Hu, Evanna. "Responsible Data Concerns with Open Source Intelligence." *Responsible Data*, 14 Nov. 2016, https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/
11. Information Sharing Environment (ISE), Program Manager "Information Sharing Environment Annual Report to the Congress" Aug. 2016, pp. 1-6 https://www.dni.gov/files/ISE/documents/AnnualReport/2016_ISE_Annual_Report.pdf
12. Jacobson, G. (2019, March 18). 5 Principles of a High Reliability Organization (HRO). Retrieved from https://blog.kainexus.com/improvement-disciplines/hro/5-principles
13. Johnson, D. B. (2019, December 23). Government information sharing efforts remain a mixed bag. Retrieved from https://fcw.com/articles/2019/12/23/information-sharing-efforts-in-government-remain-a-mixed-bag.aspx
14. Kaplan, F. M. (2014). *The insurgents: David Petraeus and the plot to change the American way of war*. New York, NY: Simon & Schuster.
15. Leander, A. (2010). The Paradoxical Impunity of Private Military Companies: Authority and the Limits to Legal Accountability. *Security Dialogue*, *41*(5), 467-490.
16. Loehrke, Ben, et al. *Ethical Decision Making with Geospatial and Open Source Analysis*. Jan. 2020, stanleycenter.org/publications/the-grayspectrum/.https://stanleycenter.org/wpcontent/uploads/2020/01/RRNWTheGraySpectrum120-web.pdf
17. McChrystal, S., Collins, T., Silverman, D., Fussell, C., Yoshikawa, M., Amacho, C., & Takatori, Y. (2015). *Team of teams*. New York, NY: Penguin Books.
18. McRaven, W. H. (2020). *Sea stories my life in special operations*. New York, NY: Grand Central Publishing.
19. Martens, K. (2002). Mission Impossible? Defining Nongovernmental Organizations. *International Journal of Voluntary and Nonprofit Organizations*, *13*(3), 271-285.
20. Office of the Inspector General of the Intelligence Community (OIGIC). "Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015." 19 Dec. 2019, pp. 1–34. https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf
21. Petraeus, D. (2009). *The Petraeus doctrine: The field manual on counterinsurgency operations*. Washington, D.C.: Aquitaine Media Corps.
22. Rajamäki, J. ; Sarlio-Siintola, S. ; Simola, J. (2018) Ethics of Open Source Intelligence Applied by Maritime Law Enforcement Authorities. In Audun Josang (Ed.) Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS 2018, 28-29 June 2018, Oslo, Norway. Academic Conferences and Publishing International Limited, 424-431. https://www.theseus.fi/bitstream/handle/10024/152174/Rajamaki_SarlioSiintola_Simola.pdf?sequence=1&isAllowed=y
23. Rajamäki, J, Simola, J (2019). How to apply privacy by design in OSINT and big data analytics?. In Cruz, Tiago; Simoes, Paulo (Eds.) ECCWS 2019 : Proceedings of the 18th European Conference on Cyber Warfare and Security, Proceedings of the European conference on information warfare and security. Academic Conferences International, 364-371. https://jyx.jyu.fi/bitstream/handle/123456789/67100/rajam%25C3%25A4ki_simola_howtoapply.pdf?sequence=-1

*Corresponding Author: **Mike Potter** .

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

24. Rosenberg, C. (Executive Producer). (July 29, 2020). *The Oath Podcast* [Audio podcast]. NBC News. https://podcasts.apple.com/us/podcast/mike-leiter-intelligence/id1461312941?i=1000486474007
25. Stanley, B. E. (2015). *Outsourcing security: Private military contractors and U.S. foreign policy*. Lincoln, NE: Potomac books.
26. Tynan, D. (2017, August 03). It's Not Top Secret: The Intelligence Community Encourages Data Sharing. Retrieved from https://fedtechmagazine.com/article/2017/08/its-not-top-secret-intelligence-community-encourages-data-sharing

*Corresponding Author: **Mike Potter** .

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.