Facilitator's Guide

Setting Your Moral Compass

A Workbook for Applied Ethics in OSINT

By Melissa Hanham

Stanley Center
FOR PEACE AND SECURITY

Table of Contents

Part One: Workbook

This workbook is designed to give you an opportunity to practice handling ethical dilemmas that are based on Real-World experiences of your OSINT colleagues in the arms control and nonproliferation world. The author interviewed 25 OSINT analysts about their ethical experience and dilemmas they faced. The framework and case studies below are based on their deepest or most frequent concerns. The majority of analysts wished to maintain their privacy, thus these case studies use fictional names for anonymity or occasionally amalgamate several concerns into one case study.

After each case study, you are asked to work through a series of steps based on the Markkula Center for Applied Ethics' recommendations.[1] You will be asked to (1) identify the dilemma or dilemmas; (2) get all the facts; (3) weigh your options; (4) test your decision with peers or imagine a hypothetical; and (5) act, learn from your decision, and evolve your thinking for next time.

[1] https://www.scu.edu/media/ethics-center/resources/making.pdf.

Introduction

This workbook is intended to support open source intelligence (OSINT) practitioners regardless of whether they work in a large organization or as a freelancer. International organizations, governments, universities, think tanks, commercial firms, and freelance consultants have all realized the opportunities that OSINT has to offer, but not all analysts have equal access to ethical guidance.

With the rise of OSINT capabilities and an abundance of data available, ethical guidance must also propagate otherwise we risk damage to the field as a whole. Those unethical actors in the field risk harm to everyone if the public sees OSINT as exploitative and dangerous. Most analysts genuinely wish to act ethically but say they don't know where to start, don't feel they have resources, or don't feel they have enough time to consider ethical frameworks.

Practicing ethics is like exercising a muscle. The case studies in this workbook are intended to help the analyst see a dilemma from multiple perspectives, distinguish between ethics and law, and practice in hypotheticals before facing real-world situations. Analysts seeking ethical guidance are not alone. Working with a colleague, reaching out to another group for red teaming, or even forming a loose network of accredited ethical practitioners are on the minds of many.

> "Educating the mind without educating the heart is no education at all."
>
> —Aristotle

Making an Ethical Decision

This workbook was inspired by an early collaboration with the Markkula Center for Applied Ethics and the Stanley Center. The Markkula Center offers many resources on its website, and its framework approach forms the basis for this workbook.[2]

Markkula identifies six major frameworks for addressing an ethical dilemma. These approaches aren't simply a checklist that you can go through to receive a correct answer. Not all approaches will apply to your situation. You may even disagree with one or more of the approaches, while some of your colleagues will agree. These approaches are best applied as different lenses from which to examine your dilemma. While they will not give you the "correct" answer, they can surface nuances that might otherwise be overlooked. If they offer you insight, use it. When the time comes, it is up to you to make the best decision, even if there is no perfect answer.

Utilitarian Approach

This approach is all about the consequences of your decision. It emphasizes reducing harm and increasing good. Since we can neither totally maximize good nor minimize harm, the goal is to find the best possible balance of good over harm. When applying it, consider who or what will benefit and who or what will be harmed.

Rights Approach

This approach focuses on the fact that all humans have innate dignity and rights. Humans have the right to choose what they do with their lives freely without harm or hindrance. These moral rights include the right to choose their own life's path, not to be injured, to privacy, and many others that remain debated in society. Some argue that nonhumans, such as animals, have rights as well. The core ethical takeaway is that it is our duty to respect others' rights.

Justice Approach

The Aristotelian origin of this approach is the notion that we should treat each other equally, though it has evolved to recognize that "equally" is not always "fairly." Thus, there are now complex societal debates on how to treat those who are historically underprivileged or overprivileged.

Common Good Approach

Another approach with a Greek origin, the Common Good Approach sees community as a good in itself. It seeks to put the benefit of the community over the individual. This approach emphasizes the common welfare of everyone and is often associated with public education, public spaces, or legal welfare systems like fire departments.

Virtue Approach

This approach marries ethics with certain virtues like honesty, courage, compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence. Markkula recommends that you ask yourself, "What kind of person will I become if I take this action?"

[2] See: https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/.

Care Approach:

The Care Approach emphasizes the interdependent relationships between the stakeholders rather than following a rigid check list or defining and calculating harm. By using empathy, try to put yourself into the shoes of each of the stakeholders and appreciate their viewpoints when it comes to assessing the interests, concerns, and agency of all parties. This approach is sometimes associated with food security, equal rights, and environmental protection as a more holistic approach to human security, for example.

Applying Ethics to Real-World Problems

Each of the six approaches above represent ethical theory, however OSINT analysts work in the real-world with imperfect data, time pressures, and resource constraints. Applied ethics offers the opportunity to take philosophical ideals and place them into a real-world context.

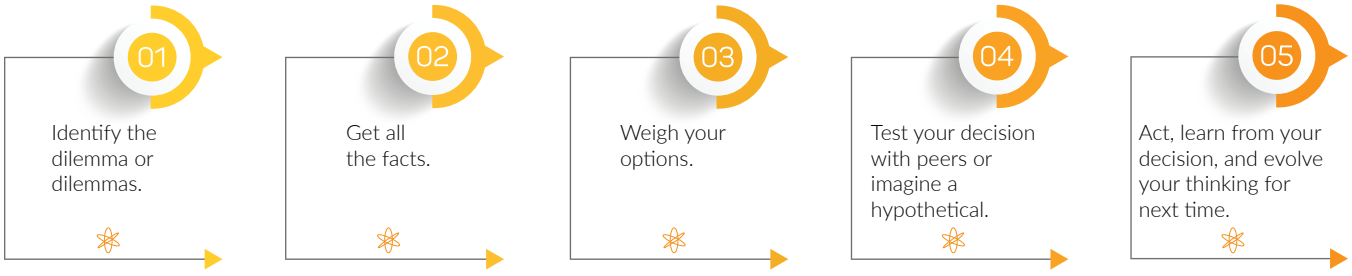
Some of the oldest examples of applied ethics include medical ethics. The Hippocratic Oath required medical physicians to swear to Greek healing gods that they would uphold ethical standards in their practice. As medicine evolves and diversifies so have the ethics associated with it.

OSINT analysts can draw much from the practice of journalism ethics. Though not uniformly alike, journalists also deal with issues such as the ethical treatment of sources, privacy, bias, and other issues.

The Markkula Framework

While there are no "correct" answers in applied ethics, the Markkula Framework developed by the Markkula Center for Applied Ethics at Santa Clara University offers a step by step approach to working through an ethical dilemma. It is important to practice thinking through ethical dilemmas, learning from them, and applying what you learned to the next time.

The framework is composed of five steps:



1. Identify the dilemma or dilemmas

First, try to identify one or more dilemmas in your situation. Putting the dilemma into your own words and writing it down can help you understand the scope of the dilemma. Ask yourself if this is truly an ethical dilemma or rather if it is a question of cost/ benefit, or even a legal issue instead. Those working on a tight budget often need to cut corners to stay on a small budget, that could be an ethical dilemma, but often is not. Similarly, many OSINT analysts confuse legal questions with

ethical questions. Laws are often rooted in ethical thinking, but not always. Regardless, OSINT analysts should be aware of the laws in their jurisdiction and the jurisdiction of those they investigate.[3]

2. Get the facts

Next, gather all the relevant facts that can help you chart a course of action. Identify the data, tools, and resources you have at your disposal. In addition to the facts of the case you are working on, think of resources you can consult or trusted allies who you can talk to.

3. Weigh your options

Most ethical decisions are not zero sum. Some dilemmas may be as simple as whether to publish data or not, but there can be variations on the theme as well. Could you publish some of the data and keep other data protected in case it is needed later? Could you request permission to publish data? Could you limit the audience of who receives the data? The majority of ethical dilemmas are not as simple as outlined above, but carefully think about various courses of action you could take in order not to miss an opportunity.

To do so, use the six ethical approaches outlined above: the Utilitarianism Approach, the Rights Approach, the Justice Approach, the Common Good Approach, the Virtue Approach and the Care Approach.[4]

4. Test your decision with peers or imagine a hypothetical

Select one of the options you have just outlined and test it out in your head. If you feel comfortable consulting with a trusted leader or peer, consider sharing it with them and listen to their feedback. Alternatively, imagine how someone you trust would react to your choice. The Markkula Center suggests that you visualize yourself announcing your decision on television.

5. Act, then learn from your decision, and evolve your thinking for next time

Now it is time to make your decision. You have already identified the dilemma and the relevant facts and tools needed to make a decision. You have also outlined several options and weighed them against each other using the six ethical approaches above. Implement your decision as best as you can and document how it turned out. Did anything unpredictable happen? Did you learn from your actions? Spend time learning about the experience and consider it the next time you face an ethical dilemma.

Case Studies

Here are five case studies you can review independently—or better yet—with other analysts. While the majority of these case studies are fictional, each one is based on a real-world situation or an amalgamation of experiences from your colleagues. After each case, you are prompted with a series of questions and activities to help you work through the ethical dynamics.

[3] See more in Part Two, page 61.

[4] See the quick reference guide in the Annex, page 92.

CASE STUDY

North Korean leader Kim Jong-Un watches the launch of an intermediate-range strategic ballistic rocket, Hwasong-12, at an undisclosed location near Pyongyang, North Korea, August 29, 2017. (Korean Central News Agency/Korea News Service via AP Photo)

DPRK Missile Image

Olivia and Jungho are second-year graduate students working part-time at the University of Alexandria. They study international security and learn about nuclear weapons and missiles in class. During the summer, they work for Professor Lee on her project to monitor North Korea's nuclear weapons program. Part of their duties are to scan Korean-language news in North Korea and South Korea to look for signs that North Korea could be developing new nuclear-capable missiles. In addition, they've been trained to log in to the university's commercial satellite imagery accounts to check locations of suspected nuclear and missile facility sites for activity. Some commercial providers offer daily imagery of locations, meaning students can check to see if anything changed since the day before. Other commercial providers provide particularly sharp details in their images. Professor Lee has become very excited that there may be a new launch in the next few days.

North Korea tested two intercontinental ballistic missiles (ICBMs) the month prior, causing public outcry from its neighbors and the United States. The rhetoric from the American president was particularly strong. While his official statement read, "The United States will take all necessary steps to ensure the security of the American homeland and protect our allies in the region," leaks from the White House indicated that he was ready to authorize preemptive strikes. The United States and South Korea performed live-fire drills within hours of each of the ICBM tests as a self-proclaimed show of force. Tensions were running high, and the news coverage had been constant for weeks.

Olivia and Jungho were practically celebrities on campus. Each had done live television and radio interviews describing the earlier ICBM tests. The university provost had specifically called to tell them how important their work was to the mission of the university. With two back-to-back ICBM tests in July, they were now on constant alert to see if there would be a third launch.

Meanwhile, the American president announced that any further threats from Pyongyang would be met with "fire and fury." Two days later he added, "Maybe that statement wasn't tough enough." The United States was regularly flying nuclear-capable bombers in the region. Most recently the president had said, "All options are on the table" when it comes to North Korea. At the same time, North Korean state media was condemning a new round of UN sanctions as well as the military exercises performed by the United States and South Korea. North Korean state media reported that the country's army would carry out a preemptive operation if there were signs of US provocation. The state even shot off three short-range missiles from Gangwon Province to demonstrate its own "resolve."

While Olivia was busy breaking down the short-range missile launches for Professor Lee, Jungho noticed some unusual vehicle activity at the Sunan International Airport in Pyongyang. As usual, he logged into his account to view fresh satellite imagery from a few dozen sites that he checked regularly. This imagery was relatively cloud-free, and he could see some new dark objects against the pale gray of an airstrip. This airstrip was away from the main runways of the civilian airport toward an area that was presumed to be for military activities. Jolted he realized that this could be the preparation for a new ICBM launch.

Jungho carefully processed the 70 cm resolution image in order to make measurements. He tried

to reduce the risk that shadows might create an artificially long measurement. He measured multiple times and averaged the measurements. The challenge with 70 cm resolution imagery is that one pixel in both directions could represent an error margin of up to 1.4 m. With all the facts in hand, he approached Olivia with his find.

Olivia was excited to see what Jungho had found after comparing images from the two dates. They could see there were several new objects on the airstrip. Hoping for even sharper images, they searched other commercial satellite imagery catalogs, but none had an image from that day. Olivia questioned whether they were expert enough to make this call and suggested they bring in Professor Lee. Jungho agreed but knew it would just be a matter of hours before other groups would be reporting the same thing. He didn't want to get scooped by another group. The information was already out there.

"Diagnosing" the preparations for a missile launch is difficult. North Korea's missiles are road-mobile, so there is usually little to no notice before one appears. It was rare, but not the first time they had seen dark boxes on an airstrip. Jungho knew that everything they saw before them signaled a potential missile launch, but he wasn't sure it couldn't signal something else, like leaving containers out temporarily to prepare for construction. He also reminded himself that this activity was happening a stone's throw from an operating civilian airport. What if they called it wrong and the US president made good on the rumors of a preemptive strike? What if they got it right?

EXERCISES

DPRK Missile Image

Help Jungho and Olivia work through their ethical dilemma.

Step 1: Identify the Dilemma(s)

Olivia and Jungho believe they have evidence that North Korea is on the brink of launching what might be an ICBM. Is it an ethical issue, and what harms could be caused and to whom?

We'll start things off with some sample answers from the author, but note that none are clearcut.

Sample answers:

1. Is this an ethical issue?

   - ☐ Yes, imminent missile launch is something the public deserves to know about, but will it cause a panic?
   - ☐ Yes, Olivia and Jungho want to make sure they provide accurate and sound information that is not misunderstood or manipulated for politics.
   - ☐ Yes, Olivia and Jungho want to make sure they do not exacerbate an already simmering conflict.

2. Are there already procedures at their workplace to guide them?

   - ☐ Olivia and Jungho are students at a university, meaning there may already be university regulations on research.
   - ☐ Olivia and Jungho work for a professor who is an expert in this field. They can turn to Professor Lee for technical and ethical guidance.

Step 2: Get All the Facts

So far, Olivia and Jungho's information is limited to one satellite image, and while they certainly see evidence that indicates a missile launch, they can't rule out something more innocuous like shipping containers or construction. This is nearly always the case. You must make a decision with limited information, just as you do in real life. There is never perfect information. Do the best you can with the information you have in the narrative. They could wait for another image to come in, but it might be too late for the missile launch.

Who will benefit or be harmed by the outcome of their decision?

Consider the following and discuss. Then rank the importance of the issues on the line to the left:

____ Could publication cause panic in Japan, North Korea, South Korea, or the United States?

____ Could publication feed the arguments of those wanting to make a preemptive strike?

____ Does it matter that the location is near a civilian airport?

____ If they don't publish it, will someone else do it anyway?

____ Can they publish in a way that is more accurate and responsible than others?

____ Could military satellites have better information than them?

____ Should they feel responsible for what others do with their information?

____ Anything else?

Who else can they consult with?

Jungho has already consulted with Olivia, and they have agreed to speak to Professor Lee. List some other types of people who might have insight that could help.

_____ _____

_____ _____

As you see from above, Jungho and Olivia have a lot of options available to them. This is not a binary choice between publishing or not publishing. They can wait, publish limited information, choose to publish with a trusted journalist with experience in the subject, or share the information with a limited audience, for example.

Step 3: Weigh Your Options

When weighing the best course of action, consider applying the Markkula Center for Applied Ethics' approach to your situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which outcome will produce the most good and do the least harm?
- **Rights Approach:** Which outcome best respects the rights of all who have a stake?
- **Justice Approach:** Which outcome treats people equally or proportionally?
- **Common Good Approach:** Which outcome best serves the community as a whole, not just some members?
- **Virtue Approach:** Which outcome leads me to act as the sort of person I want to be?
- **Care Approach:** Which outcome protects the relationships of the stakeholders and addresses the underlying causes of the dilemma?

This may be where your group has difficulty finding consensus. For example, Jungho could take the position that publishing accurate, publicly available information treats all the stakeholders equally (Justice Approach). On the other hand, Olivia could argue that the risk that the conflict escalates to war outweighs any good from informing the public (Utilitarian Approach). They are both right. The goal is to weigh the pros and cons illuminated through each of these approaches and choose a path that makes the best out of a situation that does not have a perfect solution.

Choose one of the approaches and argue for a course of action. Now argue against it.

Consider what you might do if you disagreed with a colleague or supervisor, and make a plan before it happens.

Step 4: Test Your Decision with Peers or Imagine a Hypothetical

After considering all the angles, Olivia and Jungho need to decide what to do. If they decide to publish their analysis, they could write a draft and read it out loud to themselves or to each other to see if they have mitigated some of their concerns about panic or exacerbating conflict. They should also make sure their information is accurate and any limitations of their research (such as the spatial resolution of the image) is disclosed. Technical writing can be very difficult, because you want to balance what the public needs to know without causing confusion, fear, or distrust.[5]

The Markkula Center also proposes that you imagine a hypothetical situation: If you told someone you respect—or told a television audience—which way you decided to proceed, what would they say?

If they do choose to publish, what might be important for them to emphasize in their article? Most people will only ever read the headline and first paragraph of your article. Try writing these.

As students trying to prove themselves, Jungho and Olivia may feel they need to impress Professor Lee, or prove their worth to the university and make a name for themselves. In many ways, deciding not to publish is the most difficult choice.

Try role playing to see what it feels like.

[5] See: https://www.scu.edu/ethics/all-about-ethics/how-should-journalists-report-a-scientific-study/.

Step 5: Act, Learn, Evolve

Once Jungho and Olivia have made their decision, they need to implement it effectively to ensure it has the impact they intend.

What would you do if you were the one deciding? Plan out how you would implement your decision.

Once Olivia and Jungho have implemented their decision, they have an opportunity to watch how events unfold and if they had the outcome they expected. Every ethical dilemma is a learning opportunity and a chance to help you prepare for the next one. Always try to reflect and ask yourself, "How did my decision turn out, and what have I learned from this specific situation?"

Have you ever faced an ethical dilemma where you had to act during an ongoing conflict that could be affected by your choice? What did you do? If you have not faced such a dilemma, what do you think you would do?

Final Thoughts

This is a hypothetical scenario based on a real-world event. On August 29, 2017, at 5:57 AM local time, North Korea launched a Hwasong-12 from Sunan International Airport in Pyongyang. Though not an ICBM, this intermediate-range missile flew over Hokkaido, Japan, traveling approximately 2,700 km and reaching an altitude of 550 km before splashing into the Pacific Ocean. This was the second successful test after three failed Hwasong-12 tests and was probably intended to signal that North Korea could threaten US military assets in Guam, where nuclear bombers are based. Japanese citizens received cell phone alerts about the missile four minutes after it was launched.

The characters and organizations in this case study are fictional, but a real OSINT analyst faced this dilemma.

What do you think their decision was? (Answer below)

This example helps us understand an increasingly common dynamic in which nongovernmental OSINT analysts are playing an active role during an ongoing conflict. While this is relatively new in arms control, people in the fields of conflict analysis and human rights have been addressing this issue for some time.[6]

Consider some of the ways OSINT could change the dynamics of an ongoing conflict and discuss with colleagues.

[6] See: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.

Answer: They chose not to publish, but shortly after someone else did. When asked, they said they would make the same decision if it happened all over again.

CASE STUDY

La Hague site, a nuclear fuel reprocessing plant in France, 2014. (US Department of Energy Photo)

Double Standard for the Country of Dovinda?

Dovinda is a state with a fraught history. War after war has defined its past and many territorial disputes remain unresolved. It has a robust military and very advanced scientific and technical abilities. The neighboring state of Mandan is ethnically, ideologically, and religiously antithetical to Dovinda. While not as technologically advanced, Mandan has been making recent overtures to acquire nuclear weapons and the means to deliver them.

The United States, United Kingdom, and Europe recognize the geopolitical importance of Dovinda's territory, which borders numerous sea routes and contains the largest sweet crude oil reserves in the region. Moreover, Mandan is seen as an autocratic pariah with substandard human rights practices that funds regional terrorism and breaks nuclear and missile nonproliferation treaties.

Decades ago, Dovindan scientists based at the Corshel Nuclear Complex are thought to have indigenously developed nuclear weapons despite intense pressure from the United Kingdom and United States. They have never officially tested nuclear weapons and are not considered a nuclear weapons state. Nonetheless, most believe that Dovinda has a credible nuclear deterrent, a fact that Mandan continually cites to justify its own nuclear weapons research.

Deondre is a full-time OSINT geospatial consultant who runs his own lucrative business with major contracts in the United Kingdom and United States. He regularly reviews commercial satellite imagery to provide briefings for governments, political risk firms, satellite companies, and occasionally research centers. He's built up his business over decades and is one of the most respected names in satellite imagery interpretation. Satellite imagery is still on the rise in the open source world, and his technical skills are highly sought after because few understand how to procure and use imagery, let alone identify military and nuclear activities in it.

Professor Shevchenko, a nuclear engineer based at the world-renowned University of Oxbridge, approaches Deondre for an upcoming project that would be both lucrative and prestigious. In their first meeting, Professor Shevchenko explains that she is interested in learning more about Dovinda's recent activities at the Corshel Nuclear Complex. She's extremely interested in what satellite imagery can tell her about the nuclear activities happening on the ground. Though an expert in nuclear engineering and the nuclear fuel cycle, she's never used satellite imagery and is thus interested in relying on Deondre to deliver what she hopes will be a cache of exotic data for her to write about—and maybe even make tenure on—this little-studied topic.

Deondre drums his fingers on the desk, immediately realizing that this is going to be a very political topic. The reason this topic is rarely examined is because Dovinda's nuclear program is deeply polarizing and nearly taboo in national security circles. Like India, Israel, North Korea, and Pakistan, Dovinda operates its nuclear weapons program outside of the Treaty on the Non-Proliferation of Nuclear Weapons.

Professor Shevchenko first asks what thermal data can be captured from the site, hoping to be able to estimate the capacity of the reactor. Deondre explains that the current data available to the public is limited to 100 meter spatial resolution, making it nearly impossible to monitor an object the size of the reactor. At most, they would

be able to see one pixel, and the reactor core absorbs much of the heat. Undeterred, Professor Shevchenko presses for the best possible imagery so she can see the types of equipment on site. She's seen others publish on China's, Iran's, Mandan's, North Korea's, and Russia's nuclear programs, and she knows it's possible. Deondre knows that satellite imagery of Dovinda is tightly regulated out of fear that it could be used in an attack by one of its antagonistic neighbors. Imagery of the Corshel Nuclear Complex will be a tall order.

Before accepting a contract with the University of Oxbridge, Deondre checks to see if he can even purchase recent imagery of the Corshel Nuclear Complex. Company after company refuses to sell it or even acknowledge that it's captured. While they don't explain the reason, Deondre knows that the United States and United Kingdom are the largest consumers of commercial satellite imagery and can throw their weight around. Eventually, Deondre finds recent images from a Chinese satellite company.

As Deondre prepares the images, he immediately sees signs of construction at Corshel. Construction was taking place right alongside the reactor and reprocessing facilities, and the excavation was deep. Deondre pushes back from his computer pondering his situation. On the one hand, this is a very important finding. If this were a country like Iran, Mandan, or North Korea, it would be front page news. He firmly believes that all states should be held to the same standard and knows that Professor Shevchenko would be an excellent partner to prepare the information accurately. On the other hand, there is much potential for blowback. Deondre knew others who had gotten on the wrong side of Dovinda and been harassed ever since. With most of his contracts in the United States and United Kingdom, he was loath to ruin his career and didn't have the backing of a large institution as Professor Shevchenko did.

Double Standard for the Country of Dovinda?

Help Deondre work through his dilemma.

Step 1: Identify the Dilemma(s)

Think about the differences between Deondre's legal obligations and ethical obligations in this situation. Ethics are a set of moral values that individuals decide on. Laws and regulations are codified rules used to govern a territory, state/province, or country. Some countries even apply. Some states even apply extraterritorial laws to their citizens, which they will impose even if their citizens are abroad.

While you are not obligated to be ethical (though it has many benefits!), you are required to be compliant with the law or otherwise risk a punishment from the governing authority. That being said, some laws are unethical or immoral, and people do choose to disobey them. Make sure you understand the difference.

List some of the legal and ethical considerations Deondre should pay attention to below.

Legal	Ethical

Deondre faces other pressures, like preserving his business and avoiding harassment. How would you weigh these considerations?

Step 2: Get All the Facts

Deondre has done enough preliminary work to know there is sufficient imagery to make a sound judgement, but what should he consider about those who will be most affected by the decision?

List the individuals or groups that have a stake in the outcome.

Discuss who will benefit or be harmed by the outcome of the decision.

What kinds of people might give Deondre good advice?

Step 3: Weigh Your Options

Deondre is confident in his satellite imagery assessment, but he's concerned about a number of other factors. Consider the following:

- Deondre thinks all states should be held to the same standard, but does Dovinda deserve extra consideration due to its security situation? Does Mandan?

- Deondre hasn't entered a contract with Professor Shevchenko or her university yet, so does he owe her anything?

- Dr. Shevchenko is an expert on nuclear engineering but not satellite imagery. Is there a risk she will misinterpret the data if he's not involved in its analysis?

- Neither Deondre nor Professor Shevchenko are from the region. Should they get a local opinion?

- Is intimidation an ethical consideration?

- Anything else?

What are some of the options Deondre should consider to mitigate his concerns? Don't forget that you can apply the Markkula Center for Applied Ethics's approach to the situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which outcome will produce the most good and do the least harm?
- **Rights Approach:** Which outcome best respects the rights of all who have a stake?
- **Justice Approach:** Which outcome treats people equally or proportionally?
- **Common Good Approach:** Which outcome best serves the community as a whole, not just some members?
- **Virtue Approach:** Which outcome leads me to act as the sort of person I want to be?
- **Care Approach:** Which outcome protects the relationships of the stakeholders and addresses the underlying causes of the dilemma?

Which approaches did you find the most helpful? Which did you skip and why?

Step 4: Test Your Decision with Peers or Imagine a Hypothetical

Next Deondre needs to decide what to do. What do you suggest Deondre do in light of your understanding of the case? Pretend you are Deondre and explain your decision to Professor Shevchenko.

How might Professor Shevchenko react? How might Dovinda?

How do you check your own biases when conducting OSINT investigations? List some ways below.

-
-
-
-
-
-
-

Step 5: Act, Learn, Evolve

Deondre is ready to act. What can he learn from this experience, and how can he incorporate it into resolving his next ethical dilemma?

Final Thoughts

The characters, places, and organizations in this case study are manufactured, but a real OSINT analyst faced this dilemma and wishes to remain anonymous.

What do you think the analyst decided to do? (Answer below)

Answer: The analyst didn't share the image, but did facilitate and fact check a small article on the subject. Another institution picked up on the article and published the image, which caused widespread news coverage in the region and what one senior analyst in the field called "an international incident" when other images from different companies came out.

Analysts must be cautious when understanding local languages, cultures, geography, and politics, and check their own biases.

OSINT is booming in the United States and United Kingdom but still emerging in other countries. Since neither Deondre nor Professor Shevchenko are from the region, they should consider consulting a local expert from Dovinda and Mandan.

Intimidation is a growing problem for independent OSINT analysts who don't have the protection or advice of a larger organization. Even large universities and media outlets grapple with how to protect staff from cyberattacks and other forms of digital—or in some cases, physical—harassment.

What can independent analysts do to help each other? Do you have a plan?

CASE STUDY

Avoiding Harm to a Bystander or Dupe

Irina manages a team of analysts at a research center who are working on a complex project of mapping UN sanctions-evasion activities. Much of their work takes place at the office, where they check corporate databases for business and ship records. Some of this data is free to the public from government and international organizations, and some is purchased from data vendors. Because ships may turn off automatic identification system beacons notifying their position, the analysts also purchase satellite imagery to spot if ships are off track or meeting other ships to swap cargo. If they identify a ship that is where it isn't supposed to be or potentially handling goods barred by sanctions, they immediately swing into action to understand the corporate network that supports its activity.

One of Irina's top concerns is the large quantity of data they handle related to personal information. There are almost always names, phone numbers, and addresses of individuals associated with owning a ship or being a corporate director. In addition, it can be tricky to separate entities from individuals or deal with an individual who operates in two companies, or even duplicate names. Still, her team has many techniques using photographs, geographic data, and birth dates to reduce the risk of making a mistake. Yet, Irina constantly finds herself balancing the information that is necessary to build the network while limiting the data that might expose someone to harm.

Officially, her team is not required to follow guidelines from an institutional review board, because the research is not considered human subject research, but that could change in the future. Furthemore, one of their partners—another think tank in the field—does implement a strict internal peer-review process with several rounds of internal and external review before publication.

Another concern is what to do if you identify illegal or disturbing activity that is beyond the scope of your work. One employee, Ramesh came to Irina saying he had discovered that a defense contractor had published right-wing extremist language and even threatened self-harm on a social media site, yet it had nothing to do with sanctions busting. In another case, they used information from the social media account of a suspect's mistress to identify that the suspect was in a location conducting criminal activity, but there was no indication the mistress knew about or participated in any of the illegal activity.

In a recent case, Ramesh had been tracking the owner of a vessel suspected of moving fuel from North Korea in contravention of sanctions. He identified the name in corporate ownership records and began to search for all evidence of who this person was. Based on the ship registry, the International Maritime Organisation number, utility bills, and charitable donations, Ramesh began to paint a picture of the owner. He used Google Earth to check the address. Though the ship was bought for well over $1 million, it seemed the suspected owner of the ship was a 72-year-old Cambodian man who lived in a one-room home with a metal roof in a rural village. Social media indicated he helped at a small family restaurant run by relatives.

While Ramesh was certain he had the right man, he didn't feel like things added up. Ramesh was bothered that the documentation related to the man's ownership of the vessel was handled by an intermediary, though the practice is common in the shipping business. That is to say, for all

Cathyrose Melloan/Alamy Stock Photo

intents and purposes, this man was the legal owner of the ship, but Ramesh suspected he may have been duped.

Ramesh meets with Irina to discuss their options. They first consider their legal obligations. As a European research center, they are required to be in compliance with the General Data Protection Regulation (GDPR) even though the person they are researching is based in Cambodia. As a best practice, they have already prepared an internal memo explaining how their work is carried out in the public interest under Article 6(1)(e) of the GDPR. Their memo also outlines how the data is handled and secured, and when it will be removed from their possession. This memo will come in handy if they face legal questions later.

Their country does not have a law establishing a "right of reply," though others in the region do. Right of reply is the concept that individuals or entities have the right to defend themselves against public criticism or accusations in the same venue where it was published. Usually, this concept is addressed in media outlets and publishing houses rather than research centers, but in the end they are publishing a report publicly. Some media organizations like the BBC go above and beyond the law and implement an editorial requirement for right of reply.

While they do not have a legal obligation to reach out to the man in Cambodia, Ramesh thinks they might have an ethical one, particularly if his identity was stolen or he was duped.

EXERCISES

Avoiding Harm to a Bystander or Dupe

Help Irina and Ramesh handle this ethical dilemma.

Step 1: Identify the Dilemma(s)

Irina and Ramesh have identified a specific ethical concern regarding whether they should reach out to the man in Cambodia to see if he wants to respond to the fact that he is the owner of a ship that is involved in illicit trafficking of fuel from North Korea. However, they have broader issues related to handling of data like names, phone numbers, emails, and addresses of individuals. In addition, researchers regularly come upon information that is extraneous to their investigation but may indicate separate criminal or harmful behavior. Finally, some of the data they have is not from someone directly involved in a sanctions busting but a family member, lover, or other bystander or even dupe.

Review the case and list any dilemma you think Irina and Ramesh should address. Remember that legal and ethical dilemmas are different, and mark any legal issues with "L."

- _____
- _____
- _____
- _____
- _____

Did you choose anything that is about cost or efficiency? Those aren't ethical issues but are important to OSINT analysts regardless of whether they are an individual for-profit analyst or work in a large nongovernmental organization (NGO) or university.

How would you weigh the ethical, legal, and cost priorities if you were Irina? Why?

Step 2: Get All the Facts

Regarding the fuel ship, what are the relevant facts of the case? What facts are not known? How can Ramesh gather additional information?

If Ramesh does reach out to the man in Cambodia, what steps should he take to make sure he is in compliance with his organization's rules, protects his own privacy, and protects the man's data?

Can you think of any creative solutions that would help Ramesh?

Step 3: Weigh Your Options

Ramesh has already spoken to his boss Irina, and they are now weighing options. Consider the following:

- Even if they are not obligated to give the Cambodian man a right of reply, is it more ethical to do so? Should they publish his name at all?

- Would alerting the man to the investigation potentially undermine their efforts and make it harder for law enforcement?

- If they do reach out to him, what is the best way to interact given the cultural and language differences?

- Does it matter if he knowingly owned the ship or if he was duped into it?

- What about other kinds of bystanders? What about the mistress whose social media showed potential criminal activity of her lover? Will she be at risk if they publish the data from her account? Would the ethical decision change if she were a spouse or child? What if she was a sex worker?

Apply the Markkula Center for Applied Ethics's approach to the situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which outcome will produce the most good and do the least harm?
- **Rights Approach:** Which outcome best respects the rights of all who have a stake?
- **Justice Approach:** Which outcome treats people equally or proportionally?
- **Common Good Approach:** Which outcome best serves the community as a whole, not just some members?

- **Virtue Approach:** Which outcome leads me to act as the sort of person I want to be?
- **Care Approach:** Which outcome protects the relationships of the stakeholders and addresses the underlying causes of the dilemma?Which approaches did you find the most helpful? Which did you skip and why?

Step 4: Test Your Decision with Peers or Imagine a Hypothetical

Remember that Irina is in a position of greater authority than Ramesh at this institution, but neither are at the top. Choose a time you had to bring an ethical issue to the attention of a supervisor or leader. Think about how Irina can present their plan to leadership for handling the possibility that the Cambodian man was duped into owning the ship.

Imagine you are giving advice to a colleague with the same dilemma. How would you advise them?

Step 5: Act, Learn, Evolve

Based on your decision above, how might you implement it most effectively? Consider ethical, legal, and cost factors.

What are your contingency plans?

What are your long-term plans to handle data privacy concerns and right of reply?

Final Thoughts

The characters and organizations in this case study are fictional, but real OSINT analysts faced this dilemma. They decided to reach out to the man who owned the ship but were concerned about language and cultural differences. They reached out to a major media outlet that had local knowledge, a higher standard on right of reply, and more resources than they did. The international media outlet used one of its local reporters to speak with the man, who said he had no idea a ship was purchased in his name. The man retired from working at various maritime organizations, and it seems plausible that they were the ones operating the ship using his identity. The media outlet published the report on the illicit network, and decided to publish the documents linking the man to the ship, however it also included information provided by the man.

Privacy is the number one concern among the 25 OSINT analysts interviewed for this research project. Some of these concerns are legal due to GDPR and more recent laws promulgated by federal states or even the California Consumer Privacy Act (CCPA). While legal considerations are different from ethical ones, it is still important to be aware of them in order to act accordingly.

Do you or does your organization have a privacy policy?

CASE STUDY

Season/Adobe Stock Photo

Using Sock Puppet Accounts

Carlos and Sophia work at a small but prestigious OSINT consulting firm in the United States. The firm does a mixture of due diligence on customers and employees for banks and insurance companies and also tracks nuclear proliferation for governments and international organizations. Carlos is an anti-money-laundering expert with over a decade of experience working inside and outside banks. He has worked on several key investigations relating to insider threats at banks and is generally considered to be the go-to person around the office.

Sophia is a new hire just coming from an international organization. She's an expert on proliferation threats and knows the nuclear fuel cycle inside and out. She has about five years of experience analyzing social media, news, videos, and photos to track the flow of materials that could be used in nuclear weapons programs. Sophia decides early to ask Carlos for some tips on investigations. She can already tell that the work environment at the firm is different from the storied hallways and cramped offices of her old organization.

Carlos and Sophia get a cup of coffee and start talking shop. Sophia's quick to cut to the chase. "So what are the rules here?" Carlos laughs. 'So you expected a two-inch manual on how to conduct an investigation?" He smiles, remembering the tightly controlled environment of his most recent bank job. He replies, "don't punch down, and just ask for help from your boss if you need anything." Sophia smiles, thinking she can finally put her skills to use without a ton of bureaucracy and paperwork slowing her down.

The following month, she begins to onboard her first new client. She's excited because this means she won't just be managing cases from her predecessor, and she's landing a prestigious new government contract that will impress her boss. She has the general statement of work (SOW) lined up, and she's in final talks with her point of contact, Robin, to go over the details of the contract.

Robin joins her on videoconference to discuss the contract. Sophia briefs them on the plan to collect information from social media, saying they will track groups like scientists, engineers, students, and interpreters who have public social media accounts as they travel to countries with proliferation risk. Robin interjects, "You are going to use sock puppets, right?" Sophia takes a breath, hesitating. She has never been permitted to even consider using a sock puppet account before.

Sock puppet accounts are social media accounts that do not use the owner's real name. At her old job, you used your personal social media account or maybe one representing the organization, or it didn't get investigated. Robin shuffles some papers on their desk and continues "Look, not to put too fine a point on it, but we're coming to you to get this information without tipping off proliferators that we're watching. We don't use sock puppets, but I'm under the impression that you do." Sophia nods and says, "I'll look into this," before moving on to the next part of the contract.

After the meeting, Sophia heads directly to Carlos's cubicle. "Do we use sock puppets here?" Carlos swivels around instantly. "Of course!" Sophia lowers her voice, whispering, "At my old job we were forbidden from using sock puppets. We'd get fired for impersonating someone."

"You don't have to impersonate a real person, and in fact, please don't, but it's just easier and faster."

Sophia looks at the ceiling. "I don't know, it seems unethical."

Carlos shrugs, "Hey, it's your call, but after a few years on the job, I don't want the 'bad guys' knowing who I am."

Sophia nods, but equivocates, "Yeah, but what am I supposed to do? Lie to them? Isn't that entrapment? We don't even know that they are 'bad guys.'"

"I don't lie, I just use the sock puppet to see what's on their LinkedIn profile, or like, what conferences they're Instagramming," Carlos replies.

"So, I'm just, like, supposed to tell my employees to make these accounts? How should they behave?"

"Look, you're doing them a favor. Do you want to tell your employees to connect their auntie to our work? That's unethical."

Sophia nods noncommittally. Carlos shrugs and turns back to his keyboard. "You do you, but don't mess up the contract. Once you enter the contract, we're all liable."

Sophia heads back to her office to think.

EXERCISES

Using Sock Puppet Accounts

Help Sophia work through her ethical dilemma.

Step 1: Identify the Dilemma(s)

Sophia and Carlos each have different but compelling takes on the use of sock puppet accounts.

Generally speaking, a sock puppet account is an active social media account on a site like LinkedIn, Facebook, Twitter, or VKontakte that uses a name other than the operator's real name. While some sock puppet accounts are used to impersonate celebrities and people of note for malicious or satirical purposes, they are not explicitly designed to do this. That said, sock puppets are used in malicious activities like stalking and harassment.

Social media accounts with privacy settings turned on means the public cannot see what is posted unless they are a "friend" on Facebook or a "colleague" on LinkedIn, for example. Some OSINT analysts use sock puppet accounts so they will be added as a trusted follower and be able to see information like the location, date of birth, friends or colleagues, photos, videos, scientific publications, and conference attendance of the person they are following. This data can be monitored manually, and it can be scraped and analyzed to learn things like when the person is awake, the network of their friends and colleagues, and how often they write about certain topics.

Review the case and list any dilemma you think they should address. Remember that legal and ethical dilemmas are different, and mark any legal issues with "L."

- _____
- _____
- _____

Sophia already spoke to one of her co-workers, but what other resources may be available to her inside or outside her workplace?

Inside	Outside

Step 2: Get All the Facts

Regarding the use of sock puppet accounts, what or who should Sophia consult? Check all that apply.

- ☐ Employee handbook
- ☐ Boss
- ☐ Colleagues from her previous job
- ☐ A professor of ethics
- ☐ Robin
- ☐ Robin's government agency
- ☐ Carlos
- ☐ Mom
- ☐ Firm's guide on best practices for research
- ☐ Federal laws
- ☐ State/provincial laws
- ☐ Markkula Center for Applied Ethics
- ☐ In-house counsel or compliance officer
- ☐ HR
- ☐ Berkeley Protocol
- ☐ Religious leader
- ☐ Head of the firm
- ☐ Terms of Service/Terms of Use of the social media site

Regarding forming a contract, what or who should she consult? Check all that apply.

- ☐ Employee handbook
- ☐ Boss
- ☐ Colleagues from her previous job
- ☐ A professor of ethics
- ☐ Robin
- ☐ Robin's government agency
- ☐ Carlos
- ☐ Mom
- ☐ Firm's guide on best practices for research
- ☐ Federal laws
- ☐ State/provincial laws
- ☐ Markkula Center for Applied Ethics
- ☐ In-house counsel or compliance officer
- ☐ HR
- ☐ Berkeley Protocol
- ☐ Religious leader
- ☐ Head of the firm
- ☐ Terms of Service/Terms of Use of the social media site

Some of these options may be available to Sophia and some may not. Some may be more appropriate than others. Make sure to distinguish between the ethical concerns of the sock puppet issue and the legal concerns of the contract.

Step 3: Weigh Your Options

Sophia is transitioning from the way she was conducting OSINT analysis in one organization to a new organization. Change is hard, and she is right to stop and consider her options before she commits to a course of action, especially one with a contract attached. Consider the following:

- What are the pros and cons of sock puppet accounts?
- Does it matter that the government agency supports sock puppets?
- Does it matter that the government agency is using her firm to avoid notice?
- Is there an ethical difference between impersonating a real person and creating a fictional person?
- Does it matter if someone doesn't really know how to use the settings on their social media account?
- If Sophia decides to use sock puppet accounts, should she talk to the person or try to convince them to reveal information?
- What is the difference between an agent of law enforcement and an OSINT analyst when it comes to ethics and tactics?
- Carlos argues that Sophia should not force her employees to use their real names for their own security and safety. Is he right?
- What if using a real account tips off proliferators who change their methods, making them harder to stop?

Apply the Markkula Center for Applied Ethics's approach to the situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which outcome will produce the most good and do the least harm?
- **Rights Approach:** Which outcome best respects the rights of all who have a stake?

- **Justice Approach:** Which outcome treats people equally or proportionally?
- **Common Good Approach:** Which outcome best serves the community as a whole, not just some members?
- **Virtue Approach:** Which outcome leads me to act as the sort of person I want to be?
- **Care Approach:** Which outcome protects the relationships of the stakeholders and addresses the underlying causes of the dilemma?

Take the role of Carlos and prepare your argument for using sock puppets.

Now take the role of Sophia and prepare your argument against.

The use of sock puppet accounts could be considered on a spectrum. Circle your use level.

No sock puppet	Silently viewing accounts with your sock puppet	Silently scraping data from accounts	Having conversations using a sock puppet	Suggesting illicit activity using a sock puppet

Discuss your position with a colleague.

Regarding contracts, it's best to follow the procedure established by the person responsible in your organization. If you are an independent OSINT analyst, it's worth meeting with an attorney in your jurisdiction to understand the generalities of contracts or even to make your own boilerplate language for clients, and then follow up based on specific cases as needed.[7]

Step 4: Test Your Decision with Peers or Imagine a Hypothetical

Now it's time for Sophia to make a decision and test it out. Since she needs to follow up with Robin, help her prepare a SOW based on your decision of what she should do.

Now help her prepare her remarks for her next conversation with Robin.

What should she do if Robin—the client—doesn't agree?

[7] For more information on handling contracts when ethical issues are at stake, see the facilitator's guidebook and curriculum, stnl.cr/osint.

Have you ever faced a situation like this? If you face it again, what would you do?

Step 5: Act, Learn, Evolve

Based on your decision above, help Sophia write a policy for her employees so they understand the boundaries of the decision.

Do you or does your organization have a policy on sock puppets? If so, describe. If not, how would you write a policy and make it easily understood and followed?

Final Thoughts

This case study represents an amalgamation of several OSINT analysts' views on sock puppet accounts. While the characters and organizations are fictional, the perspectives represented are real. OSINT analysts are keenly aware that sock puppets can be an ethical gray zone. Several managers of OSINT analysts expressed concern about both requiring their employees to use their real accounts or requiring them to use sock puppets. Employees are aware of what they are being asked to do and are not always sure what to do if they don't agree with an OSINT method.

One thing that may be overlooked by OSINT analysts are the terms of use of the social media sites they are using. Some sites, like Facebook, prohibit the use of the site with a name that is not on your ID card.[8] Sites may also prohibit the scraping of data from their site, so it's worth checking the "Terms of use" or the "Terms of service" section of the website.

At one point, Sophia refers to "entrapment." Typically, the term "entrapment" only refers to an activity of a law enforcement agency.[9] It's a common misperception that an individual can "entrap" someone. That being said, OSINT analysts should remember that their role and responsibilities are not the same as law enforcement agents.

Some analysts in the private sector have expressed concern that their clients may misuse their work or use their data beyond its intended purposes. Depending on the jurisdiction, this may represent a low legal risk to you. However, if you are concerned about the ethical handling of the analysis or data you produce as an OSINT professional, there are many good options beyond turning down the contract in the first place.

The head of one OSINT company said he was approached by a European government to collect telephone GIS data on migrants coming from North Africa and the Middle East. Ostensibly, it was for the purpose of providing services, however, he felt strongly that it would be used to target the world's most vulnerable. He said that if his firm had been asked to target the smugglers who were trafficking in migrants, he might have had a different answer. As the head of his own organization, he could make the call to turn down the contract and lose business, but not everyone can. He noted that other organizations did the work instead.

The legal remedies for a client misusing your data are limited and likely inadequate. Depending on the jurisdiction, you could receive monetary compensation if you can demonstrate destruction of data or damage to your reputation, but this can be quite expensive and difficult to prove. It's also possible that a court might rule that the data be removed from your client, but as we all know, data is easy to copy, whether it is on a private drive or on the internet. Lawsuits of this nature are expensive and can take years to conclude.

---

[8] See: https://www.facebook.com/help/112146705538576.

[9] For a US perspective, see: https://www.nolo.com/legal-encyclopedia/entrapment-basics-33987.html#:~:text=Entrapment%20is%20a%20defense%20to,someone%20to%20commit%20a%20crime.

CASE STUDY

Megaworks/Adobe Stock Photo

Unintentional Harm to Employees

Chunhua is program director of the chemical, biological, radiological, and nuclear (CBRN) program at the Paris School of Economics. She's an expert on nuclear security and manages a team of three analysts who cover a portfolio running the gamut of weapons of mass destruction, as well as the risk that nonstate actors could acquire them. It's a tightly stretched team that works hard and always delivers. Chunhua's proud that she put together such a great team of diverse talents and knowledge. She knows she's tough and often brags about how hard-core her team is when other colleagues present on more abstract deterrence and compellence topics at the university.

Sani is one of her analysts, and his focus is on preventing nonstate actors from acquiring CBRN materials for the purpose of terrorist attacks. He's an expert on Boko Haram, as well as the larger Islamic State. He's a valuable asset to the team because he speaks Hausa, English, and French fluently, though he is quite reserved and rarely speaks at all.

Amira is another analyst who jokes that she's the failed doctor her parents always wanted. Rather than patch up rich ski bums like her dad, she wanted to make a difference with political science and switched out of pre-med. She puts her medical skills to use by analyzing videos of people experiencing trauma after a purported chemical weapons attacks.

Antoine rounds out the team. The youngest of the group, he's an intern and student. He mostly collects data from French nationalist sites and is writing a paper on the rise of right-wing extremism in France.

One afternoon, Antoine leaps up from his desk, slams shut his laptop, and storms off. He doesn't return for the rest of the day. Chunhua noticed that he's been somewhat disrespectful and curt around the office. She chalks it up to being a bit inexperienced and maybe partying too late. He does sometimes come into the office looking like he never went to bed. She makes up her mind to talk to him about it next week after she finishes editing the final draft of their most recent report on the Islamic State West Africa Province (ISWAP) and radiological sources. It's a big project with a ton of data and it's due next week. She'll probably work all weekend.

Several months ago, she tasked Sani with collecting evidence of ISWAP attacks in areas near Nigeria's research and medical reactors. News coverage has been sketchy, so she's been asking for original source material like photos, videos, and satellite imagery of attacks on convoys, military bases, and even humanitarian outposts. She's concerned not so much about the nuclear reactors themselves but about the transport of fissile material on some of the road routes. There's no imminent sign of Boko Haram expressing interest in radiological weapons, but the Islamic State is a concern and ISWAP could try to acquire fissile material.

Sani's been great. He comes in early and works quietly all day. He's captured a trove of data with Antoine, so much that Amina's been pulled in for the last few weeks. There were hours of videos to comb through. Some of it is Boko Haram and some is ISWAP; none of it is pretty. Because of the similarities between the groups, the analysts have been looking for flags or insignias that differentiate the groups. ISWAP is thought to be less viscious with civilians than Boko Haram, but there are still cell phone videos of rape and

People attend a funeral for those killed by suspected Boko Haram militants in Zaabarmar, Nigeria, Sunday, Nov. 29, 2020. Nigerian officials say suspected members of the Islamic militant group Boko Haram have killed at least 40 rice farmers and fishermen while they were harvesting crops in northern Borno State. The attack was staged in a rice field in Garin Kwashebe, a Borno community known for rice farming. (Jossy Ola/AP Photo)

bombing victims to comb through. Each piece of evidence was geolocated and tied to a geographical place on a map.

Amina is her usual cheerful self. She even shares some tips she uses when looking at videos of chemical weapons attacks. She says she takes regular breaks and eats sugar. The men mostly shrug it off, but Chunhua says they should do whatever they need to do to get the job done.

The next day Amina knocks on Chunhua's door and asks to talk. Amina looks nervous and explains that she doesn't want to undermine her colleagues, but she's a little worried about them. Sani barely talks to her anymore, and Antoine keeps blowing his top. Chunhua's manager instincts kick in immediately, and she pulls out a notebook. "No, no, it's nothing serious," says Amina. "I think they are getting burned out from the attack videos. I feel it too sometimes."

"In fact, there is one video that makes me really uncomfortable. I know we need to document all the evidence, but I kind of wanted to ask if we could withhold the rape victim videos from publication. Those women will get shunned if they are identified."

"It's not just this project, but you know—well—Antoine has found some white nationalist propaganda in his own neighborhood, and Sani's—well—I think he's just getting too withdrawn. Even for him. Did you know he has a brother in the Nigerian Army?"

Chunhua thanks Amina for bringing this to her attention and promises to take action.

Unintentional Harm to Employees

Help Chunhua handle the situation in the office.

Step 1: Identify the dilemma(s)

Chunhua feels terrible. Is it ethical for her to ask her employees to look through this violent content? It must take a toll.

Review the case and list any issues that you think she should address.

Chunhua works at a university; what resources might be available to her? What if she ran her own start-up instead of a big university??

University	Start-up

Step 2: Get All the Facts

Regarding Sani, what facts are known or not known? How can Chunhua sensitively inquire and provide him support if he is feeling trauma?

Regarding Antoine, what facts are known or not known? How can Chunhua sensitively inquire and provide him support if he is feeling trauma?

Can you think of any creative solutions that would help Chunhua limit harm to her employees?

Step 3: Weigh Your Options

Chunhua has already heard from Amina, and she probably needs to speak to Sani and Antoine before making up a plan for handling harmful content in the office. Consider the following:

- What are the power dynamics in the office?
- What are the gender dynamics in the office?
- What are the cultural dynamics in the office?
- What evidence needs to be published and what can be withheld regarding the rape victims?
- Should Sani's brother's safety be considered?
- Should they be concerned about reprisals to their office from far right extremists?

Apply the Markkula Center for Applied Ethics's approach to the situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which outcome will produce the most good and do the least harm?
- **Rights Approach:** Which outcome best respects the rights of all who have a stake?
- **Justice Approach:** Which outcome treats people equally or proportionally?
- **Common Good Approach:** Which outcome best serves the community as a whole, not just some members?
- **Virtue Approach:** Which outcome leads me to act as the sort of person I want to be?
- **Care Approach:** Which outcome protects the relationships of the stakeholders and addresses the underlying causes of the dilemma?

Which approaches did you find the most helpful? Which did you skip and why?

Step 4: Test your Decision with Peers or Imagine a Hypothetical

Imagine you are Chunhua, and write out the first paragraph of what she might say to Sani.

Do you or your organization have a policy on trauma? If so, describe it. If not, write a proposal for one.

Step 5: Act, Learn, Evolve

Based on your decision above, how might you implement it the most effectively? Consider ethical, legal, and cost factors.

How might Chunhua onboard a new employee regarding the issue of traumatic media consumption?

What are your long-term plans to handle traumatic exposure to media?

Final Thoughts

The characters and organizations in this case study are fictional, but the scenario is based on an amalgamation of comments made by real OSINT analysts who wish to remain anonymous. In addition to the ethics around requiring employees to view violent content, one analyst felt that his family abroad may have been put in danger by the activities of his larger institution. Additionally, one analyst called for a greater focus to be placed on gender in conflict and to prevent revictimization of those most vulnerable.

OSINT analysts want to do good, but they might not realize the negative impact of violent digital content on their mental health, particularly until universities begin to adopt curriculum on this subject. Every person is different, and gender and culture can influence how people are affected and how willing they are to come forward or seek healthy coping skills.

Best practices dictate that resources should be put in place for employees before beginning a project with violent media. New employees should be trained as they are onboarded, and then regular training should be available as necessary.[10]

Do you or does your organization have a trauma policy?

[10] For additional information on vicarious or secondary trauma, identifying its signs, and mitigating it's harm, see the facilitator's guidebook and curriculum, stnl.cr/osint.

CASE STUDY

DedMityay/Adobe Stock

Buying Data on the Dark Web

In perhaps one of the biggest OSINT coups yet, Bellingcat partnered with CNN, Der Spiegel, and the independent news website the Insider to identify the network of chemical weapons experts inside the Russian Federal Security Service (FSB) as they trailed political opposition leader Alexei Navalny. During this time period, Navalny was poisoned with a chemical weapons agent in the class known as Novichok.

On August 14, 2020, Alexei Navalny flew from Moscow to Novosibirsk, Russia, where social media show him meeting volunteers and posing with fans. On the 17th, he continued to Tomsk, where he held meetings with volunteers of his campaign center and election candidates. He stayed at the Xander Hotel while filming videos for his center over two days.

On August 20, he left his hotel for the Tomsk Airport to return to Moscow. A photo posted on social media shows him drinking something from a paper cup in the Vienna Cafe inside the Tomsk Airport about 40 minutes ahead of his flight, according to a clock on the wall. Minutes later, another social media user posts a photo of him on an airport bus. His plane took off at 8:06 AM local time.

@maxseddon

According to his travel companion, he began to feel sick immediately after takeoff. The plane made an emergency landing at Omsk Central Airport. He can be heard groaning on a video taken on a smartphone inside the plane as someone wearing a yellow vest and blue medical gloves walks by. Another video shows him being carried in a sling-like stretcher into a yellow ambulance. He was then taken to the Omsk Emergency Hospital Number 1.

While the hospital in Omsk said there was no evidence of poisoning, Navalny was transferred to a hospital in Berlin for treatment two days later at the request of his family. German doctors then confirmed poisoning by a Novichok agent. By September 9, German doctors were able to bring Navalny out of a medically induced coma and later off of a mechanical ventilator. Navalny eventually returned to Russia, where he was arrested and imprisoned.

According to Bellingcat:

> "A German military laboratory, two independent European labs and the Organization for the Prohibition of Chemical Weapons (OPCW) all identified the toxin as a nerve agent belonging to the Novichok group. The OPCW identified the toxin as a

> cholinesterase inhibitor structurally resembling the known Novichok variants, but one that was not included in the list of banned nerve agents updated after the Skripal poisoning in 2018. This implied that the agent used on Navalny was of a more recent, previously unknown type."[11]

Bellingcat's investigation showed that Navalny had been followed by FSB agents with chemical and medical expertise on over 30 flights in 2017 during his presidential election campaign and 2019-2020 leading up to his August 20 poisoning. They even theorize that there may have been an attempt weeks earlier in Kaliningrad. Bellingcat was further able to identify three men who trailed him to Novosibirsk on August 14, and then to Tomsk where he was poisoned: Alexey Alexandrov, 39, Ivan Osipov, 44—both medical doctors—and Vladimir Panyaev, 40. They were supported by at least five more FSB agents, some of whom also followed Nalvany to Omsk after the emergency landing. According to telephone records obtained by Bellingcat, the team communicated with each other throughout the trip, as well as when Navalny left his hotel for the airport, and at the suspected time of the poisoning.[12]

In order to put together the network of FSB agents, identify them by name, locate them by nearest cellphone tower, and learn of their medical and chemical experience, Bellingcat purchased leaked or stolen data from one of Russia's many data markets on the dark web. For only a few hundred euros worth of cryptocurrency, they were able to buy telephone records with geolocation data, passenger manifests, and residential data. Aside from the data brokers paying off low-level employees for data, there are huge batches of leaked or stolen data readily available via torrent. According to Eliot Higgins, the head of Bellingcat, they meticulously cross-referenced each piece of data they bought or found online with names, dates of birth, license plates, passport numbers, and other information to verify it was accurate.[13]

Bellingcat maintains a semiprivate chat network on Slack, where Higgins says, there was "lots of debate and discussion as they realized how much [data] they could get."[14] Higgins said that when weighing the ethics of purchasing data from brokers in Russia, he felt it was acceptable because of the "scale and scope" of the case. In fact, he felt it might have been unethical not to use it because of the potential to stop future political assassinations.[15] He also said this and other high-profile cases caused Bellingcat to really professionalize its work and scale up in size. It has adopted internal supervisory reviews like media organizations and has joined the Dutch press association. Going a step further, Bellingcat is now working on meeting an OSINT standard that could make its work admissible in court. At the time of print German courts are accepting OSINT analysts as expert witnesses.

---

11 For more on their analysis: https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.

12 See: https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.

13 To see Bellingcat's methodology: https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology.

14 Interview with author.

15 Interview with author.

EXERCISES

Buying Data on the Dark Web

Step 1: Identify the Dilemma(s)

Eliot Higgins knew that buying data on the dark web was ethically gray, but he felt it was worth it to stop future political assassinations.

List the pros and cons of buying data on the dark web.

Pro	Con

If you think purchasing data on the dark web is acceptable, what kind of data is OK to buy and what kind is not?

OK	Not OK

Step 2: Get All the Facts

If you were thinking about purchasing data from the dark web, what kind of facts would you want to know before making an ethical decision?

Whom or what might you consult to get more facts?

Step 3: Weigh Your Options

This decision's already been made, but pretend you are talking with Eliot Higgins and his team in the fall of 2020. Consider the following:

- What kind of data is being purchased?
- Who is the seller, broker, and/or other intermediary?
- How might the proceeds of the purchase be used?
- Who are the other buyers?
- How can you be sure the data is authentic? (Don't forget the method above)

Apply the Markkula Center for Applied Ethics's approach to the situation. You can choose one approach or several, or even rank the approaches to help you make a decision.

- **Utilitarian Approach:** Which option will produce the most good and do the least harm?
- **Rights Approach:** Which option best respects the rights of all who have a stake?
- **Justice Approach:** Which option treats people equally or proportionally?
- **Common Good Approach:** Which option best serves the community as a whole, not just some members?
- **Virtue Approach:** Which option leads me to act as the sort of person I want to be?

Which approaches did you find the most helpful and why? Which did you skip and why?

Step 4: Test Your Decision with Peers or Imagine a Hypothetical

Pretend you are writing a policy for yourself or your organization. What might you include?

Explain your plan to your boss or a senior colleague below.

Step 5: Act, Learn, Evolve

Based on your decision above, how might you implement it most effectively? Consider ethical and legal factors for your jurisdiction. Consider how employees will know the rules and how to enforce the decision.

What are your contingency plans?

Final Thoughts

All the names, places, and techniques in this case study are real! Thanks to Bellingcat for sharing its thinking on its ethical and technical processes.

Remember that ethical and legal decisions are different. The author is not expert enough to judge the legality of Bellingcat's decision to purchase stolen or leaked data from the dark web. Keep in mind that laws for the buyer and the seller may be different based on their jurisdictions. For those in the United States, the US Department of Justice has provided a memo on the subject.[16]

Do you or does your organization purchase data? What is the policy on data that is stolen or leaked regardless or whether it was purchased?

[16] See: https://www.justice.gov/criminal-ccips/page/file/1252341/download.

Part Two: Facilitator's Guidebook

Introduction

Part two consists of a facilitator's guidebook and an accompanying slide deck to help an instructor, leader, or facilitator train open source intelligence (OSINT) analysts to practice identifying and handling ethical dilemmas independently, distinguish between legal and ethical dilemmas, and feel empowered to use resources on ethical decision making.

Our goal is to critically evaluate moral considerations as they apply to research on arms control, disarmament, nonproliferation, and international security policy.

Whom is this guidebook for?

This guidebook is intended to help a leader, manager, peer, or an instructor facilitate a group of OSINT analysts in learning applied ethics based on the exercises associated with the case studies in the accompanying workbook. If you are reading this guide, you are likely preparing to lead a group.

If you are an individual OSINT analyst, first work through the accompanying workbook at your own pace and refer to this guide for a deeper dive on some of the concepts after you do.

Why should you use this guidebook?

Our goal is to critically evaluate moral considerations as they apply to research on arms control, disarmament, nonproliferation, and international security policy. OSINT education and training is on the rise, but few courses include the ethical dimension of the trade.

If you already train analysts on technical skills, applied ethics should be given equal weight. It is recommended that you

set aside paid work time for analysts to train. This allows you to set the tone for your group and emphasize the seriousness with which you or your organization takes ethics, and it allows your team to focus.

How should you use this guidebook?

This guidebook will help you identify resources and prepare a lesson plan for your cohort. It will also help you lead a group through the six case studies in the accompanying workbook and suggests activities that can be done in a small-group setting to cement the main concepts.

Your Trainees

While some analysts are extremely technically adept, they may not have considered the ethical impacts of their work. For these types of analysts, it is best to draw their attention to the question, "Even if you *can* do it, *should* you do it?" In the early days of OSINT, as capabilities surged, many analysts (this author included) chose to focus on the technical breakthroughs of OSINT rather than the ethical implications.

Some OSINT analysts have backgrounds in journalism, philosophy, or law enforcement, and may already have concrete ideas about applied ethics. To the extent their ideas are in line with your organization's, try to make them allies in the training. They can provide valuable insights and experience to the group. They also contribute to the ethical culture within the team.

Some analysts will take to these concepts quickly, and others may struggle. Trainees will also bring varied perspectives—including cultural, generational, and gender perspectives—to the exercise. These viewpoints may affect how they engage with the material. These nuances are worth discussing openly with the group. Acknowledging, respecting, discussing, and learning from those perspectives is part of the exercise.

Some of your team may struggle to distinguish between what is and is not ethics. The greatest misconception is that ethics is derived from derived from the law, religion, or cultural norms. We will explore these issues later, but try to prepare your team to set aside some of their preconceived ideas about ethics and approach the training with an open mind.

On the off chance that an analyst does not take the training seriously or continually expresses ideas contrary to your goals, take them aside early. Explain why the training is being organized and the risks you see if ethical practices are neglected, and listen to their points so they feel heard.

Tips for an Inclusive Discussion

The analysts in your group may come from different backgrounds and experience levels. They may work independently or in a large institution. Your group may include individuals of different genders, races, religions, ages, national origins, and cultures. This is wonderful. You've already built a team that will be more aware of and resistant to biases, but it will be necessary for you to connect with all the analysts so they feel heard and accepted and contribute their perspective to the group. To do this:

- **Build trust:** Building trust is key to having your group be introspective, open up, and make themselves vulnerable. Nobody wants to be seen as unethical, especially in front of their peers or boss. Assure participants that everyone faces ethical dilemmas and

that there is rarely a "correct" answer. As a facilitator, you have a duty to empower discussion rather than shut down viewpoints. Actively intervene if you observe members ganging up on a minority opinion. Use statements that debate the idea, never the person. The ultimate goal is for your colleagues to feel comfortable coming forward with an ethical dilemma rather than hiding it or guessing because they are afraid of judgment.

- **Identify your own biases:** Everyone has them, so the best we can do is be aware of them and act accordingly. As you prepare to train, think about some of your own biases and be ready to handle them when you speak with your group. You may even want to address this head-on and ask everyone in the group to do this.
- **Adjust your speaking style:** If you are outgoing, that's wonderful, but not everyone is. Be sure to spend as much time listening to your team's discussion as you do lecturing. There are no absolutes in ethics, and so you should also remove expressions like, "Everyone knows that…" or "You would be crazy to…" Talk these scenarios out instead.
- **Reach everyone:** Not everyone likes to speak, so find a way to connect with the quieter participants through their written work, small-group activities, or during a meeting break. Maybe even give them notice that you would like to call on them in the next section so they are prepared. Make sure you do not always call on the same outspoken person. Pay attention to race and gender, for example, when calling on analysts for participation.
- **Avoid microaggressions:** A microaggression is a statement or action that is an indirect or unintentional instance of discrimination. Some common microaggressions are interrupting women and minorities, asking people who look different from you where they are from, or commenting on the exoticness of someone's appearance. If you truly need this information, then apply it evenly across the group, perhaps having each person introduce themselves. If you do not know the gender expression or sexual orientation of your group members, don't make an

The ultimate goal is for your colleagues to feel comfortable coming forward with an ethical dilemma rather than hiding it or guessing because they are afraid of judgment.

assumption. Listen to how they speak about themselves and follow their lead, or ask the whole group. If you intend to address people with their titles (Dr., Amb., Ms., etc.) rather than their given names, be sure you apply that equivalently for all participants.

Building Resources for Yourself or Your Organization

Though this training is intended to be a practical way to exercise applied ethics, you may want to go a step further to organize ethics resources, revise practices, or even develop or adopt a code of ethics for yourself or your organization.

The key to starting this process is to get buy-in from leadership early on. If your organization already does an internal risk assessment, you may want to add ethics to the list. If not, you may want to identify hazards of unethical behaviors in your work. Will your reputation be damaged? Will your research or findings be rejected? All of this could lead to loss of clients or funding. Where unethical behavior crosses into prohibited behavior, you may lose access to websites or data, or even face legal consequences. Also, consider ethical behavior as a possible opportunity. If you can show your work is accurate and ethical, you may attract clients and funding.

Consider the options below as initial steps for enhancing your ethical practices.

Organize Resources

Education and awareness are essential for ethics, but it can be tough to get started. Assembling written resources or a reading list can make it easier for you, your organization, and your peers to do independent study, join ethics discussions, and reference the literature.

Consider materials that help users understand sources of ethics, contextualize ethical dilemmas common to working with OSINT, and relate to the ethics experiences of professional communities like journalism or government intelligence gathering. Some resources drawn from the field of applied ethics are on pages 66 and 67.

Revise Review Processes

Your colleagues and your network are valuable resources. It's important to be able to seek ethics guidance from, discuss dilemmas with, and justify decisions to peers and trusted colleagues. Consider how you can update your analytical or editorial practices to bring focus and intentionality to those discussions.

Peer review and red teaming are already widely accepted as best practices for research, though they rarely include a focus on ethics. Some of the case studies will explore how individuals or groups explored resources for ethical guidance. In some cases, you may even seek ethical or legal guidance outside your organization or strategically partner with a group that has more resources. Many of the individuals and organizations interviewed for this project expressed a desire to collaborate on ethical guidance. Make sure to keep your group thinking of new creative ways to collaborate.

Develop Codes

Creating your own code of ethics is no simple feat. Start by examining some other codes of conduct. At the time of publication of this guidebook, C4ADS and Open Nuclear Network had codes of ethics for their OSINT analysts on their websites. The citations are below. Make sure analysts as well as leaders are consulted in the drafting. You

may also wish to consult with human resources and/or compliance officers when you consider enforcement of your policy. Peer review from other individuals or organizations is another way to get feedback for the final draft.

If you develop a code, make sure it is well understood. Circulate the code and give people time to read it and ask questions. Incorporate it into the training you are doing now. Tell colleagues what to do if they have questions or suggestions. Let people know if their workflow will need to change to accommodate any new policies. Be clear about whether the policy is voluntary or mandatory and what the consequences are if they are not followed.

Recommended Reading

Here are some materials you may wish to review as you train OSINT analysts or build out your own policies. These may also be incorporated into a syllabus.

Ethics with OSINT

- Stanley Center for Peace and Security. *The Gray Spectrum: Ethical Decision Making with Geospatial and Open Source Analysis*, January 2020, https://stanleycenter.org/publications/the-gray-spectrum.
- Benjamin Loehrke and Aida al-Kaisy, et al. *Feeling the Burden: Ethical Challenges and Practices in Open Source Analysis and Journalism*, January 2022, https://stanleycenter.org/publications/ethics-osint-analysis-journalism.
- Office of the United Nations High Commissioner for Human Rights and Human Rights Center, University of California, Berkeley, School of Law, *Berkeley Protocol on Digital Open Source Investigations*, 2020, https://human-rights.berkeley.edu/programs-projects/tech-human-rights-program/berkeley-protocol-digital-open-source-investigations.

Ethics and Ethical Decision Making

- Markkula Center for Applied Ethics. *A Framework for Ethical Decision Making*, November 8, 2021, https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making.
- Fanny Verrax. "Beyond Professional Ethics: GIS, Codes of Ethics, and Emerging

Challenges," in *Technoscience and Citizenship: Ethics and Governance in the Digital Society*, ed. Ana Delgado, Cham: Springer, 2017, https://www.researchgate.net/publication/312078831_Beyond_Professional_Ethics_GIS_Codes_of_Ethics_and_Emerging_Challenges.

- Congressional Research Service. "CIA Ethics Education: Background and Perspectives," June 11, 2018, https://sgp.fas.org/crs/intel/IF10906.pdf.
- Hannah Ellis. "How to Prevent, Identify and Address Vicarious Trauma—While Conducting Open Source Investigations in the Middle East," in the Middle East," Bellingcat, October 18, 2018, https://www.bellingcat.com/resources/how-tos/2018/10/18/prevent-identify-address-vicarious-trauma-conducting-open-source-investigations-middle-east.

Codes of Ethics

- Society of Professional Journalists. "SPJ Code of Ethics," last revised September 6, 2014, https://www.spj.org/ethicscode.asp.
- Urban and Regional Information Systems Association. "GIS Code of Ethics," last revised April 9, 2003, https://www.urisa.org/about-us/gis-code-of-ethics.
- C4ADS. *Our Ethics: A System of Lighthouses in Uncertain Times*, 2020, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5f7f35d-1fee52224071c5c07/1602173434959/C4ADS+Ethics_Statement.pdf.
- Open Nuclear Network. "Code of Ethics," Last revised June 25, 2020, https://www.oneearthfuture.org/program/open-nuclear-network/code-of-ethics.

Books

- Fred Brown, ed. Media Ethics: A *Guide for Professional Conduct*, 5th ed. Indianapolis: Society of Professional Journalists, 2020.
- Randolph Pherson and Richards Heuer. *Structured Analytic Techniques for Intelligence Analysis*, 3rd ed. Thousand Oaks, CA: SAGE, 2021.
- Amy Zegart. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton, NJ: Princeton University Press, 2022.

Lesson Plan

Here is a sample lesson plan you can use to facilitate discussions with your peers, staff, or students. It is intended to be modular. Timing is illustrative of a half-day training. You can adapt or rearrange the modules, run the training in segments, scale the timing, and adjust the materials to suit your needs.

Sample Agenda

While this agenda is designed for approximately 4.5 hours of work time, it is strongly recommended that you add break time to allow participants to stay comfortable while absorbing new material. Please download an editable version that you can adapt to your own purposes.

Timing	Module
10 minutes Plenary	**Warm-Up** – Welcome all participants and warm up by asking them about why ethics matter in their work. Solicit examples of dilemmas they have faced. – **Sample exercise:** pair off and discuss a time you faced an ethical dilemma with your partner.
5 minutes Plenary	**Introduction** – Lay out goals for the training. – Explain why case studies are useful. – Walk through agenda.
5 minutes Plenary	**What Is Ethics?** – What is ethics? – What is NOT ethics? – What is applied ethics?
10 minutes Plenary	**Ethical Lenses** Walk participants through the Markkula Center's ethical frameworks: – Utilitarianism Approach. – Rights Approach. – Justice Approach. – Common Good Approach. – Virtue Approach. – Care Approach. – Pause for questions and clarification.

10 minutes Plenary	**Ethical Decision Making** – Examine the five-step process of handling an ethical dilemma · Step 1: Identify the dilemma(s). · Step 2: Get all the facts. · Step 3: Weigh your options. · Step 4: Test your decision with peers or imagine a hypothetical. · Step 5: Act, learn, evolve.
20 minutes Groups	**Exercise** – Ask participants to break into groups of four to five people. – Present an ethical dilemma related to your work and tell them to examine it using the approaches they just learned.
5 minutes Plenary	**Questions**
15 minutes	**Break**
5 minutes Group	– Introduce a Case Study – Divide into groups of three to five participants – Introduce the narrative – Provide instructions for the exercise
60 minutes Group	**Case Study—Round 1** – Groups analyze the case and choose one or more ethical frameworks to structure their deliberation..
5 minutes Per Group	**Debrief—Round 1** – Each group presents to the plenary, explaining the decision they made and how they arrived at it. – If you have five groups you can ask each group to describe what they did for one of the five steps of the frameworks. Ask the other participants if there are variations or other feedback.
15 minutes	**Break**
60 minutes Group	**Case Study—Round 2** – Groups use the five-step process outlined in the workbook, individually or as a team, as described in the section

20 minutes Per Group	**Debrief—Round 2** – Each group presents to the plenary, explaining the decision they made and how they arrived at it. – If you have five groups you can ask each group to describe what they did for one of the five steps of the frameworks. Ask the other participants if there are variations or other feedback.
20 minutes Plenary	**Debrief** – Reconvene all groups into one plenary. – Discuss with participants what they learned through the exercise. – Discuss how the exercise made them think differently about practices with their own work.
20 minutes Plenary	**Next Steps and Conclusion** – Discuss what resources, guidance, or processes participants see as valuable for enhancing their ethical practices, the practices of the organization, or the conduct of peers in their community.
Total: approximately 4.5 hours of work time	

Suggested Set Up and Materials

- A room that can be arranged with plenary seating as well as breakout sessions for small-group work. This could be one large room, with several clusters of tables, for example.
- A projector and screen if using slides.
- A flipboard and markers for each group.
- Pencils and notepads for participants.
- A laptop or laptops and internet connection for activities that require online work. If not available, choose the alternative activity.
- A copy of Markkula Framework for participants. (see Annex on page 92)
- The workbook or the case studies you intend to use on for the participants.
- This guidebook for yourself and any other facilitators participating.

Background and Tone Setting

Participants will have varied levels of awareness of and experience with ethics. Before the exercise, you will need to define key terms, establish baseline understandings with your participants, and walk through the process of ethical decision making.

Warm-Up

Start with a skeptical position. Ask your group to name some of the reasons we might consider ethical behavior in our work.

- Why should we care about ethics when we have so many other priorities?
- What's more important—being right or having people believe you?
- How can we weigh arms control over other social priorities like privacy?
- What if others are unethical?

Write answers on a whiteboard or use a chat function online.

Get to know your group. If participants struggle, start by discussing medical or journalism ethics, then make the link back to arms control research ethics.

Main Concepts

This training program uses the Markkula Center for Applied Ethics' framework for ethical decision making.[17] Take the time to familiarize yourself with the framework. It would be a good idea to share the framework with or give physical copies of it to your trainees. The Markkula Center's website also has a wealth of resources that might be useful to you as you build resources and familiarize yourself with the topic.

The case studies in this training program are derived from the strongest or most frequent concerns of the OSINT analysts interviewed by the author. These are:

- Privacy.
- Avoidance or mitigation of harm.
- Distinguishing between what is legal and what is ethical.

Key Terms

Ethics

A well-founded set of standards of right and wrong that prescribe how humans ought to behave.[18]

Ethical dilemma

A situation where a choice must be made between courses of action each of which might transgress a moral principle.

Applied ethics

An interdisciplinary application of ethics to practical decision making, including in domains like journalism, medicine, law, engineering, business, and technology.

[17] Markkula Center for Applied Ethics. A *Framework for Ethical Decision Making*, November 8, 2021, https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making.

[18] Sheila Bonde, Paul Firenze, et al., A *Framework for Making Ethical Decisions*, Brown University Science and Technology Studies, last revised May 2013, https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions.

Open source information

Publicly available information that any member of the public can observe, purchase, or request without requiring special legal status or unauthorized access.[19]

Approaches to Ethics

Ethical decision making requires being able to explain choices between simply right and wrong. It requires nuanced thinking that is not zero sum. You can approach those choices from a variety of perspectives. There is no inherent answer of what is or is not ethical. To help inform those choices, philosophers have developed systems of ethics that provide lenses—along with logics that explain those perspectives.

There is no inherent right or wrong approach to ethics.

It's expected that individuals will apply different approaches to the same ethical dilemma and justify different actions as ethical. That's OK.

These exercises aim to get teams familiar with these sources of ethics—and get individuals to explain their own ethical decisions using these approaches.

For this training program, and in keeping with the Markkula Framework, we'll use some of the most prominent approaches to ethics. Participants should familiarize themselves with these six approaches. During the exercises, they will be asked to apply these approaches as they justify decisions.

Utilitarianism Approach

This approach is all about the consequences of your decision. It emphasizes reducing harm and increasing good. Since we can neither totally maximize good nor minimize harm, the goal is to find the best possible balance of good over harm. When applying it, consider who or what will benefit and who or what will be harmed.

Rights Approach

This approach focuses on the fact that all humans have innate dignity and rights. Humans have the right to choose what they do with their lives freely without harm or hindrance. These moral rights include the right to choose their own life's path, not to be injured, to privacy, and many others that remain debated in society. Some argue that nonhumans, such as animals, have rights as well. The core ethical takeaway is that it is our duty to respect others' rights.

Justice Approach

The Aristotelian origin of this approach is the notion that we should treat each other equally, although it has evolved to recognize that "equally" is not always "fairly." Thus, there are now complex societal debates on how to treat those who are historically underprivileged or overprivileged.

Common Good Approach

Another approach with a Greek origin, the Common Good Approach sees community as a good in itself. It seeks to put the benefit of the community over the individual. This approach emphasizes the common welfare of everyone and is often associated with public education,

[19] Office of the United Nations High Commissioner for Human Rights and Human Rights Center, University of California, Berkeley, School of Law. *Berkeley Protocol on Digital Open Source Investigations*, 2020, 6, https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.

public spaces, or public welfare systems like fire departments.

Virtue Approach

This approach marries ethics with certain virtues like honesty, courage, compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence. When faced with an ethical dilemma, ask yourself, "What kind of person will I become if I take this action?"

Care Approach

The Care Approach emphasizes the interdependent relationships between the stakeholders rather than following a rigid checklist or defining and calculating harm. By using empathy, try to put yourself into the shoes of each of the stakeholders and appreciate their viewpoints when it comes to assessing the interests, concerns, and agency of all parties. This approach is sometimes associated with food security, equal rights, and environmental protection as a more holistic approach to human security, for example.

Process

Ethical decision making takes practice. A structured approach to it can make it easier to understand core concepts and develop routines. In time, ethical decision making should feel second nature, allowing analysts to more easily anticipate, recognize, and process ethical dilemmas. The Markkula Framework is a practical tool for developing those skills and for managing real-world dilemmas.

You should have ready and familiarize yourself with the steps of the Markkula Framework.

Five steps when facing an ethical dilemma:

- Identify the dilemma or dilemmas.
- Get the facts.
- Weigh your options.
- Test your decision with peers or imagine a hypothetical.
- Act, then learn from your decision, and evolve your thinking for next time.

For the following exercises, trainees will need to interrogate their case studies by following the five steps of the framework and consider the related questions and activities in the workbook.

Distinguishing between Ethical and Legal Issues

One of the most prevalent misunderstandings is the conflation of what is legal and what is ethical. Laws are a system of rules and regulations enforced by a government or authorities. While many laws and regulations are based on ethical principles, not all are. Many civil rights leaders have broken laws they deemed unethical. Work with your participants to understand when an issue is legal versus when it is ethical.

Provide clear instructions to employees on how to handle legal and ethical questions within your organization. Please also be aware of the "terms of service" or "terms of use" on websites, online data, or software. Even if it is not illegal per se, you have entered a contract with another party and may have your accounts or IP blocked if you are using the site in contravention of its stated rules.

When OSINT analysts were interviewed by the author, privacy was the issue that worried them the most. In part this was due to relatively new laws promulgated throughout Europe and by the European Union. Privacy is both an ethical and a legal consideration. When in doubt about the law, you could align your work policies to err on the side of ethics, or you can consult an attorney able to provide advice on the laws of your jurisdiction. The General Data Protection Regulation (GDPR) is notable not only because it regulates activities that happen in Europe but also the data of Europeans no matter where it is being used.

Understanding Your Jurisdiction

Every jurisdiction or territory will have laws and regulations you should be aware of. Spend time researching laws in the places you live or work in, travel to, or trade with. Countries may have extraterritorial laws that apply to their citizens no matter where they go.

Sometimes the difference between what is legal and what is illegal is intent. Try documenting your intent in a memo before starting your work.

Check the laws and regulations of your jurisdiction to understand the implications for OSINT related to:

- Privacy.
- Copyright.
- Hacking.
- Accessing/sharing national security information.
- Export control.
- Right of reply.
- Purchasing stolen or leaked information.
- Impersonation.
- Recording conversations.
- Extraterritorial research limits based on citizenship.

Though not a legal requirement, you may also be obligated to adhere to the terms of an agreement to use things like social media websites, databases, and software or risk losing

access or even being sued. Often referred to as "terms of service" or "terms of use," these conditions should be available publicly and/or at the time of registration or purchase. Common OSINT activities that may be impacted by terms of service include:

- Impersonation/sock puppet accounts.
- Scraping data, including text, photos, videos, and files.
- Accessing back-end or developer features without permission.
- Sharing passwords or licenses.
- Distributing data or new data derived from the site's data.
- Using a VPN.
- Accessing a site or using software in specific blocked or banned territories.

Universities frequently have an institutional review board or other administrative body established to protect the rights and welfare of human research subjects recruited to participate in studies. While the origin of these bodies is rooted in biomedical research, be aware that it may stretch into research practices for interviewing subjects or handling personal data.

Ethics within the Workplace

Throughout the research and interview process that informed these training tools, OSINT analysts expressed a concern about the inability to eliminate harm from their work. As you will see from the case studies, it is not possible to eliminate all harm. Our goal is to reduce harm as much as possible.

Considering harm within your workplace should be a high priority for your organization. The health, safety, and security of your employees is changing with the new digital dimensions of OSINT work. While most workplaces have a safety checklist for physical injuries in the office, they may not be ready for the new kinds of injuries brought about by the digital media within OSINT analysts work. Common concerns are cybersecurity of work as well as personal information, harassment, and intimidation either online or in person, and the consumption of violent and harmful media during information analysis.

Cyber and Physical Harassment

Resource constraints can make harassment a difficult problem to deal with. Your first duty is to inform analysts of the risks they may be taking on. These can include cyberattacks on their personal email, bank, and social media accounts. Encourage them not to reuse passwords and to use multifactor authentication so that if one of their passwords is stolen it cannot be used to access multiple accounts. You can also encourage them to keep personal and work devices separate.

If your employees travel internationally, make sure the data and software they are carrying across the border complies with local laws. In almost all cases, border agents have the right to search and potentially seize data and equipment. While you may work in a country with liberal laws on freedom of speech, an employee's destination may have strong national security laws that prohibit certain data, including documents, images, or information pertaining to military topics from being brought in.

Women, Black and Indigenous people, and People of Color, in particular, face harassment online. This can come from individual trolls or vast networks of bots seeking to discredit research. Make sure employees know they can come to you if they are experiencing harassment digitally or in person. Make a plan ahead of time for employees to contact you if they are detained or questioned by law enforcement, and check your local authorities on how to report crimes against you, your employees, or your organization.

Trauma

Viewing graphic or violent content in the form of photos or videos is widely accepted to be linked to vicarious trauma (sometimes called secondary trauma) or eventually posttraumatic stress disorder (PTSD). However, studies disagree on the prevalence of trauma cases. Law enforcement agencies, in particular, have seen a link to vicarious trauma and burnout during digital investigations of child pornography rings, for example.[20] Journalists are also facing a dramatic increase in digital eyewitness accounts, which means those affected by trauma are no longer limited to reporters in the field.

While large organizations may have already recognized the risk to employees and invested in limiting harm, small organizations generally lack financial resources for staff counseling or reducing the number of hours a day staff are exposed to violent content.

Signs of vicarious trauma include:

- Experiencing lingering feelings of anger, rage, and sadness.
- Becoming overly involved emotionally.
- Experiencing bystander guilt, shame, feelings of self-doubt.
- Loss of hope, pessimism, cynicism.
- Distancing, numbing, detachment.
- Use of alcohol, drugs.[21]

Eyewitness Media put together a comprehensive report based on a large survey of journalists, academics, and human rights/humanitarian nongovernmental organizations (NGOs) working with digital media. It found:

> "This type of repeated exposure can, in particular, have an intensified impact upon those who have specific skills sets or knowledge, and who are seen as the only ones in the organisation who understand certain technical tools, have certain knowledge or speak a particular language."[22]

In OSINT settings, that can mean the people with language skills or technical skills operating photo and video software to geolocate the camera or take measurements in the photo.

[20] George W. Burruss, Thomas J. Holt, and April Wall-Parker. "The Hazards of Investigating Internet Crimes against Children: Digital Evidence Handlers' Experiences with Vicarious Trauma and Coping Behaviors," *American Journal of Criminal Justice* 43, no. 3 (2018): 433-447. https://doi.org/10.1007/s12103-017-9417-3.

[21] British Medical Association. "Vicarious Trauma: Signs and Strategies for Coping," January 17, 2022, https://www.bma.org.uk/advice-and-support/your-wellbeing/vicarious-trauma/vicarious-trauma-signs-and-strategies-for-coping.

[22] Dubberley, Sam, Elizabeth Griffin, and Haluk Mert Bal. *Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline.* EyeWitness Media Hub, (2015). 25. https://first-draftnews.org/wp-content/uploads/2018/03/trauma_report.pdf.

The Eyewitness Media report firmly sees vicarious trauma as a management issue. The more senior the employees, the less likely they are to see violent digital images, yet they are the ones with the resources and power to implement mitigation strategies. "Management often does not fully acknowledge the negative impact that viewing traumatic eyewitness media can have on the individual because they incorrectly assume that their staff are fine, safely tucked up in headquarters 'merely' looking at a computer screen." Only 30 percent of journalists surveyed by Eyewitness Media said they would be comfortable coming forward to a manager about trauma. Even fewer NGO employees were willing to come forward.[23]

Creating a supportive work culture is critical to avoiding employee turnover, burnout, or worse. Managers should be active rather than passive in ensuring that employees have:

- Regular breaks.
- Someone they can talk to even if it is not a therapist or social worker.
- The opportunity to defer or delay a project.
- Limited hours devoted to consuming violent content.

Because employees, particularly junior employees, are so reluctant to come forward, leadership must make this a priority.

On Contracts

More than once, OSINT analysts expressed concern that they were asked to do something unethical by their client, either for simplicity's sake or because the client wished to evade their own institution's regulations. However, they felt they were legally bound to go through with the work.

The best time to understand a contract is before you sign it. While most of us don't have the time or patience to review every contract we come across, any contract describing your work is worth reading and understanding in careful detail. Any experienced party dealing with contracts will accept that you will want time to review it, so resist the argument that you should sign it when it is first presented to you.

[23] Dubberley, Making Secondary Trauma, 41.

The easiest way to resolve an ethical question regarding contract work for a client is to define the boundaries of your work prior to signing the contract in a statement of work. In any contract you are signing to perform work for a business, organization, or government, you are being hired for your expertise. It is unlikely that the contract will be detailed enough to outline how you do your work. Nonetheless, if you have ethical concerns about the method by which the client expects you to collect data or what happens to the data after you collect it (two of the most common concerns for OSINT analysts), it is best to codify it in the contract.

Contracts vary from jurisdiction to jurisdiction, but here are some common issues to look out for:

- **Governing Law or Jurisdiction:** There should be (but is not always) a place in your contract that identifies the controlling law in the event of a dispute. It should identify the territory, state/province, or the country whose laws control the contract for any disputes regarding your contract. It may go so far as to identify the courthouse where you resolve any legal disputes. The laws of this jurisdiction will also control the enforceability of the contract (see below).
- **Vagueness:** When a contract term is not clear, is the vagueness held against the person who drafts the contract or the person who signs it? Often, any vagueness is held against the person who drafted the contract, in order to encourage careful language. Some contracts will have language indicating both parties drafted or bargained for this specific contract in order to avoid vagueness being held against the drafter of the contract. If your contract has such a clause, make sure the terms in it are precise enough for you and an outside reader who is not technically knowledgeable but may be adjudicating a dispute.
- **Entire Agreement or 'Four Corners' Clause:** It is common in negotiating contracts to have several drafts and multiple emails or phone calls discussing possible provisions. In order to minimize misunderstandings, contracts will often state that the final contract is the entire agreement and disclaim any statements made before the contract is signed or any previous drafts. This provision will likely also disclaim any statements made contemporaneously as well. The laudable goal is that signatories shouldn't need to look outside the four corners of the final signed contract to resolve any disputes.
- **Unenforceability:** It is surprisingly common for contracts to have terms that are unenforceable under the jurisdiction's law. This may be due to an outdated contract template or plain ignorance of the law. A heavily flawed contract may be voidable (able to be canceled by one of the parties) or void (unable to be enforced by any party). If your client is asking you to do something illegal, then it is likely the contract is unenforceable. Nonetheless, try to prevent this from happening by creating a good contract from the start.

Case Studies

The next section refers to the specific case studies in the accompanying workbook. It is intended to give the facilitator additional context, activities, and resources for the case studies.

DPRK Missile Image

This case deals with OSINT analysis of satellite imagery ahead of a possible missile launch in North Korea. This is the first case study in this Facilitator's Guidebook (though you may choose to omit it or reorder it), thus it includes some sample answers to start participants off in the workbook. Regardless of which case study you choose, make sure to reinforce the five-step process of handling an ethical dilemma.

Main Ideas

- **Ongoing conflict:** This case takes place during an international crisis. While it is rare for OSINT analysts to face these kinds of situations, the potential consequences of their ethical decisions are higher during times of crisis. Digitalization of information means it spreads faster than ever before, and during an ongoing conflict, decisions are made quickly with the best information that is available at the time.
- **Manipulation of data for political goals:** While an analyst may be trying to make a decision based on fact, their data may be used by others to advance a political goal. Stick to the facts and try to write analysis so that even an extreme actor could not manipulate it.
- **Civilians and bystanders:** When conducting analysis, consider civilians in or around a place where a military activity is happening. Take them into consideration for your ethical decision. In this case, it was the civilian airport with regular flights to Beijing.

- **Explaining technical limitations:** Stating the limits of your data is another important idea to focus on. Practice explaining the method or technology you are using in clear and simple language. Also, list uncertainty margins using clear, simple language.

Optional Activities

In addition to working through the questions and activities listed after the case study and reinforcing the five-step method from the Markkula Framework, you may wish to engage in one of these sample activities.

1. Create a debate around the different ethical approaches. Assign the participants to represent (a) Utilitarian, (b) Rights, (c) Justice, (d) Common Good, (e) Virtue. Ask them to make arguments for their approach in this case. After a representative of each group has spoken, ask another participant from each group to make a rebuttal.
   - 5 min Organize a representative/group for each approach (this can also be done ahead of time).
   - 10 min Representatives/groups review case and form arguments.
   - 10 min Each representative presents a timed, two-minute argument.
   - 10 min Representatives/groups prepare a rebuttal.
   - 10 min Representatives make a timed, two-minute rebuttal.
   - 10 min Facilitate a discussion on which points made the most sense.
2. Get volunteers to play the roles of Jungho and Olivia. Flip a coin or use a random number generator to choose whether they decide to publish or not. Have the volunteers act out their decision to publish or not publish and the reasoning behind it. You play the role of Professor Lee and press them on whether they have taken all the main concepts into account and completed all the steps of the Markkula process.
   - 5 min Select volunteers (this can also be done ahead of time).
   - 10 min Prepare dialogue (or have them prepare during a break time).
   - 10 min Dialogue.
   - 10 min Group discussion and questions.

Page 80 photo: Korean Central News Agency/Korea News Service via AP.

Double Standard for the Country of Dovinda?

This case regards the fictional country of Dovinda and the construction activity at its reactor and reprocessing site.

Main Ideas

1. **Double standards**: When considering which projects to pitch, don't forget some of the lesser-studied areas. We shouldn't limit ourselves to the national goals of the country we operate in. Self-reflection is also important.

2. **Bias:** Every person has innate bias based on their lived experience. Recognize your bias and strive to overcome it. Diversify your contacts, seek peer review, and use techniques like structured analysis in your methodology.

3. **Local knowledge:** Most OSINT analysts are based in the United Kingdom and United States, but they study regions far afield. Be sure to partner with colleagues who speak local languages and understand the cultural and political context.

4. **Fear of harassment or reprisals:** Deondre was concerned that he might face harassment from agents of the Dovindan government, or even lose business.

5. **Legal versus ethical:** This case study gives participants a chance to practice identifying the difference between legal and ethical considerations.

Optional Activities

In addition to working through the questions and activities listed after the case study, you may wish to engage in one of these sample activities.

1. Have the group work quietly to circle or highlight all the parts of the case that deal with legal issues. Have one or more volunteers explain why they chose them and whether they are also ethical considerations and why.
   - 10 min Reviewing and circling.
   - 10 min Volunteers speak to the group to identify legal and/or ethical considerations.
2. Split the group into two smaller groups and have one represent the Dovindan point of view and the other represent the Mandan point of view. Ask them to state their position on publishing or not publishing the analysis and satellite image with particular attention to the concept of harm.
   - 5 min Organize groups (this can be done ahead of time).
   - 10 min Groups meet separately to build their case.
   - 5 min Dovindan case.
   - 5 min Mandan case.
   - 15 min Group discussion on harm, the stakeholders, and how to adopt different perspectives.

Page 82 photo: US Department of Energy .

Avoiding Harm to a Bystander or Dupe

This case focused on a manager who leads a team of analysts investigating sanctions-busting activities in shipping.

Main Ideas

1. **Privacy:** This team deals with publicly and commercially available information about individuals. When pieced together it can reveal personal information like the person's full name, age, and address. Try to limit harm by documenting all data with original sources but withholding some information if it is not immediately important to your publication.

2. **Right of reply:** This concept is not prevalent in every country. It states an individual or entity has the right to defend itself against public criticism or accusations in the same venue where it was published. Even if there is no law, consider applying it.

3. **Beyond the scope:** Multiple researchers said they uncovered evidence of harmful behavior or criminal activity that was beyond the scope of their research. Make a plan ahead of time of how you might handle these situations. Identify local resources that can help you if you see someone engaged in criminal activity or expressing self-harm or violent threats online.

4. **Bystanders:** It's important to think about all the kinds of stakeholders in your research. Some bystanders are more vulnerable to abuse if they are identified. Please be especially cautious identifying victims of crime or those who would be shunned or harmed by society.

Optional Activities

1. Ask your participants to use a computer to locate all the information they can about themselves. They do not have to share any information if they do not want to. If some of the participants have difficulty, suggest a site like https://www.familytreenow.com/.

   If your organization uses commercial databases from LexisNexis or Thomson Reuters, tie this exercise into your typical workflows.

   - 20 min — Independent research on their computer or phone.
   - 10 min — Group discussion about what was found and how it impacts them.

2. Have the group break into smaller groups and ask them to consider which issues they would address in a privacy policy to protect the rights of bystanders. How would this affect workflows, and what are the tradeoffs? Ask a representative from each group to present the group work.

   - 5 min — Form groups (this can be done ahead).
   - 20 min — List concepts and tradeoffs using whiteboards or a shared document online.
   - 5 min (each) — Have a representative of each group present their policies.
   - 10 min — Engage in a discussion on the merits of each of the policies.

Using Sock Puppet Accounts

This case focuses on a small OSINT firm where Carlos and Sophia debate using sock puppet accounts for OSINT research.

Main Ideas

1. **Sock puppets:** Sock puppets are a common tool used by OSINT analysts to monitor private social media accounts. Some argue that it's no different than using a VPN for your IP address. Others say the social media users have an expectation that their data is limited according to their settings. Sock puppets can be abused, and they can also be prohibited by the terms of service of a social media site.

2. **Outsourcing:** Governments and international organizations hire OSINT analysts to do work that may be politically sensitive or considered below the evidentiary threshold of their own intelligence gathering. Make a plan ahead of time of what you will or won't do if you want to take these contracts. Pay specific attention to concerns about the method by which data is collected and what happens to the data after it is turned over. Make your contract explicit to avoid ethical conundrums later.

3. **Employee security:** Organizations have an ethical duty to their employees. Sock puppet accounts have the benefit of keeping a user's identity anonymous, thereby protecting them from potential harassment.

Optional Activities

1. Have participants break into pairs. One person plays the government client Robin, and the other plays the manager Sophia, who does not want to use sock puppets. Each pair should discuss the pros and cons of sock puppets and then design a contract that meets both their needs.

   - 20 min — Independent research on their computer or phone.
   - 5 min — Break into pairs (this can be done ahead). Display the slides showing common clauses in contracts on the screen.
   - 10 min — Prepare your main points separately.
   - 20 min — Negotiate the terms of a hypothetical contract (it can be simple but should contain a statement of work and any clauses that you think will help mitigate ethical concerns).
   - 15 min — Poll how many were able to conclude a contract and follow up with discussion, thoughts, and questions.

2. Have participants go for a walk with a partner (if possible) and discuss if they have ever used a sock puppet and to what extent. Post the graphic of the spectrum of use on the slides before people go.

   - 5 min — Break into pairs, view the spectrum graphic.
   - 20 min — Walk or stretch your legs while discussing sock puppet accounts.
   - 10 min — Report back to the group on highlights.

Page 86 photo: Season/Adobe Stock.

Unintentional Harm to Employees

This case focuses on a group of researchers investigating terrorist attacks near civilian reactor sites in Nigeria. Through the course of their investigation, they have to view a large number of violent videos and images involving beheading, rape, and bombing scenes.

Main Ideas

1. **Unintentional pressure to perform:** Supervisors and leaders can unintentionally send mixed signals to employees. In this case, Chunhua brags about how "hard-core" her team is, and she told them "they should do whatever they needed to do to get the job done." Chunhua didn't mean to compromise their health, but it may have been hard for her employees to know. Leaders should embrace ethics and self-care, otherwise their employees will feel it is not a priority.

2. **Creating a safe and proactive culture:** Everyone handles trauma differently, and gender and culture can play a role in how willing people are to come forward and seek help. Set up resources and guidelines ahead of projects that require consumption of violent content.

3. **Identifying symptoms and intervening early:** Circulate a list of symptoms to managers and staff working on projects that involve violent content. Provide opportunities for employees to take a

break or change work duties or schedules without shame. Better yet, proactively set breaks and limit screen time for violent content.

4. **Privacy for victims:** Amina raised a valid concern about the rape victims. Since the project only needs to map out the locations of attacks, they can easily withhold the video itself from their publications. Protecting the privacy of victims should be paramount.

Optional Activities

1. Display the slide listing the symptoms of vicarious trauma. Ask the group to review the case and underline any passages that indicate a team member could have been experiencing trauma.
   - 10 min Review case and underline.
   - 10 min Discuss in group and write answers on a whiteboard or online chat.
2. Have the participants break into two smaller groups. Flip a coin or use a random number generator to assign one team to present the case for exposing employees to violent content and the other team to present the case against.
   - 5 min Break into groups (this can be done ahead).
   - 15 min Small group discussions.
   - 5 min Pro.
   - 5 min Con.
   - 2 min Pro rebuttal.
   - 2 min Con rebuttal.
   - 10 min Group discussion.

Page 88 photo: Megaworks/Adobe Stock.

Buying Data on the Dark Web

This case chronicles Bellingcat's investigation of an attempted assassination of Alexey Navalny using leaked data purchased from a broker.

Main Ideas

1. **Using leaked or stolen data:** Ever since the 2010 WikiLeaks incident, OSINT analysts have been debating the use of leaked or stolen data. The US government went so far as to prohibit federal employees from reading any of the leaked cables.

2. **Purchasing data from unknown entities:** One of the issues to consider is who you are paying and what the proceeds of the sale are going to. If you are unintentionally funding crime or worse, you should be wary. Checking sanctions lists can be one tool, but much of the data is sold by brokers.

3. **Verification of data:** In addition to the legal and ethical concerns, good research dictates that the sources must be verifiable. Without the US government authenticating any of the WikiLeaks cables, they could never be fully verified. In this case, Bellingcat cross-referenced each piece of data across multiple data sets.

4. **Law versus ethics:** Bellingcat justified its decision with the argument that the good from reducing the risk of future assassination attempts outweighed any risk from purchasing leaked or stolen data. In addition to the legal discussion you are having here today, be aware of legal implications in your own specific jurisdiction.

Optional Activities

1. Have participants break into pairs. One person plays the data broker and the other the purchaser. Have a dialogue over the purchase of stolen telephone records.

   - 5 min — Break into groups (this can be done ahead of time).
   - 10 min — Negotiate over the phone records.
   - 15 min — Group discussion: Who concluded a purchase and who did not? Why? Were the groups that purchased data able to minimize harm?

2. Focus on Step 5 of the process. How did Bellingcat's experience inform your own ethical decision making? Ask for volunteers to share their perspectives.

   - 15 min — Writing or thinking individually.
   - 15 min — Discussion in the group.

Page 90 photo: DedMityay/Adobe Stock.

Annex

Six Ethical Approaches

UTILITARIANISM APPROACH

This approach is all about the consequences of your decision. It emphasizes reducing harm and increasing good.

RIGHTS APPROACH

This approach focuses on the fact that all humans have innate dignity and rights. Humans have the right to choose what they do with their lives freely without harm or hindrance.

JUSTICE APPROACH

This approach enshrines that we treat each other equally, although it has evolved to recognize that "equally" is not always "fairly."

COMMON GOOD APPROACH

This approach sees community as a good in and of itself. It seeks to put the benefit of the community over the individual.

VIRTUE APPROACH

This approach marries ethics with certain virtues like honesty, courage, compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence.

CARE APPROACH

This approach emphasizes the interdependent relationships between the stakeholders rather than following a rigid checklist or defining and calculating harm.

Markkula Framework's Five Steps When Facing an Ethical Dilemma

01 Identify the dilemma or dilemmas.

02 Get all the facts.

03 Weigh your options.

04 Test your decision with peers or imagine a hypothetical.

05 Act, learn from your decision, and evolve your thinking for next time.

Slide Decks

Located at stnl.cr/osint.

A Framework for Ethical Decision Making

Reprinted with permission of the Markkula Center for Applied Ethics

Original source: https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/

We all have an image of our better selves—of how we are when we act ethically or are "at our best." We probably also have an image of what an ethical community, an ethical business, an ethical government, or an ethical society should be. Ethics really has to do with all these levels—acting ethically as individuals, creating ethical organizations and governments, and making our society as a whole more ethical in the way it treats everyone.

What Is Ethics?

Ethics refers to standards and practices that tell us how human beings ought to act in the many situations in which they find themselves—as friends, parents, children, citizens, businesspeople, professionals, and so on. Ethics is also concerned with our character. It requires knowledge, skills, and habits.

It Is Helpful to Identify What Ethics Is Not.

Ethics is not the same as feelings. Feelings do provide important information for our ethical choices. However, while some people have highly developed habits that make them feel bad when they do something wrong, others feel good even though they are doing something wrong. And, often, our feelings will tell us that it is uncomfortable to do the right thing if it is difficult.

Ethics is not the same as religion. Many people are not religious but act ethically, and some religious people act unethically. Religious traditions can, however, develop and advocate for high ethical standards, such as the Golden Rule.

Ethics is not the same thing as following the law. A good system of law does incorporate many ethical standards, but law can deviate from what is ethical. Law can become ethically corrupt—a function of power alone and designed to serve the interests of narrow groups. Law may also have a difficult time designing or enforcing standards in some important areas and may be slow to address new problems.

Ethics is not the same as following culturally accepted norms. Cultures can include ethical and unethical customs, expectations, and behaviors. While assessing norms, it is important to recognize how one's ethical views can be limited by one's own cultural perspective or background, alongside being culturally sensitive to others.

Ethics is not science. Social and natural science can provide important data to help us make better and more-informed ethical choices. But science alone does not tell us what we ought to do. Some things may be scientifically or technologically possible and yet unethical to develop and deploy.

Six Ethical Lenses

If our ethical decision making is not solely based on feelings, religion, law, accepted social practice, or science, then on what basis can we decide between right and wrong, good and bad? Many philosophers, ethicists, and theologians have helped us answer this critical question. They have suggested a variety of different lenses that help us perceive ethical dimensions. Here are six of them:

The Rights Lens

Some suggest that the ethical action is the one that best protects and respects the moral rights of those affected. This approach starts from the belief that humans have a dignity based on their human nature per se or on their ability to choose freely what they do with their lives. On the basis of such dignity, they have a right to be treated as ends in themselves and not merely as means to other ends. The list of moral rights—including the rights to make one's own choices about what kind of life to lead, to be told the truth, not to be injured, to a degree of privacy, and so on—is widely debated; some argue that nonhumans have rights, too. Rights are also often understood as implying duties—in particular, the duty to respect others' rights and dignity.

The Justice Lens

Justice is the idea that each person should be given their due, and what people are due is often interpreted as fair or equal treatment. Equal treatment implies that people should be treated as equals according to some defensible standard such as merit or need, but not necessarily that everyone should be treated in the exact same way in every respect. There are different types of justice that address what people are due in various contexts. These include social justice (structuring the basic institutions of society), distributive justice (distributing benefits and burdens), corrective justice (repairing past injustices), retributive justice (determining how to appropriately punish wrongdoers), and restorative or transformational justice (restoring relationships or transforming social structures as an alternative to criminal punishment).

The Utilitarian Lens

Some ethicists begin by asking, "How will this action impact everyone affected?"—emphasizing the consequences of our actions. Utilitarianism, a results-based approach, says the ethical action is the one that produces the greatest balance of good over harm for as many stakeholders as possible. It requires an accurate determination of the likelihood of a particular result and its impact. For example, the ethical corporate action, then, is the one that produces the greatest good and does the least harm for all who are affected—customers, employees, shareholders, the community, and the environment. Cost/benefit analysis is another consequentialist approach.

The Common Good Lens

According to the common good approach, life in community is a good in itself, and our actions should contribute to that life. This approach suggests that the interlocking relationships of society are the basis of ethical reasoning and that respect and compassion for all others—especially the vulnerable—are requirements of such reasoning. This approach also calls attention to the common conditions that are important to the welfare of everyone—such as clean air and water, a system of laws, effective police and fire departments, health care, a public educational system, or even public recreational areas. Unlike the utilitarian lens, which sums up and aggregates goods for every individual, the common good lens highlights mutual concern for the shared interests of all members of a community.

The Virtue Lens

A very ancient approach to ethics argues that ethical actions ought to be consistent with certain ideal virtues that provide for the full development of our humanity. These virtues are dispositions and habits that enable us to act according to the highest potential of our character and on behalf of values like truth and beauty. Honesty, courage,

compassion, generosity, tolerance, love, fidelity, integrity, fairness, self-control, and prudence are all examples of virtues. Virtue ethics asks of any action, "What kind of person will I become if I do this?" or "Is this action consistent with my acting at my best?"

The Care Ethics Lens

Care ethics is rooted in relationships and in the need to listen and respond to individuals in their specific circumstances, rather than merely following rules or calculating utility. It privileges the flourishing of embodied individuals in their relationships and values interdependence, not just independence. It relies on empathy to gain a deep appreciation of the interest, feelings, and viewpoints of each stakeholder, employing care, kindness, compassion, generosity, and a concern for others to resolve ethical conflicts. Care ethics holds that options for resolution must account for the relationships, concerns, and feelings of all stakeholders. Focusing on connecting intimate interpersonal duties to societal duties, an ethics of care might counsel, for example, a more holistic approach to public health policy that considers food security, transportation access, fair wages, housing support, and environmental protection alongside physical health.

Using the Lenses

Each of the lenses introduced above helps us determine what standards of behavior and character traits can be considered right and good. There are still problems to be solved, however.

The first problem is that we may not agree on the content of some of these specific lenses. For example, we may not all agree on the same set of human and civil rights. We may not agree on what constitutes the common good. We may not even agree on what is a good and what is a harm.

The second problem is that the different lenses may lead to different answers to the question "What is ethical?" Nonetheless, each one gives us important insights in the process of deciding what is ethical in a particular circumstance.

Making Decisions

Making good ethical decisions requires a trained sensitivity to ethical issues and a practiced method for exploring the ethical aspects of a decision and weighing the considerations that should impact our choice of a course of action. Having a method for ethical decision making is essential. When practiced regularly, the method becomes so familiar that we work through it automatically without consulting the specific steps.

The more novel and difficult the ethical choice we face, the more we need to rely on discussion and dialogue with others about the dilemma. Only by careful exploration of the problem, aided by the insights and different perspectives of others, can we make good ethical choices in such situations.

The following framework for ethical decision making is intended to serve as a practical tool for exploring ethical dilemmas and identifying ethical courses of action.

A Framework for Ethical Decision Making

Identify the Ethical Issues

1. Could this decision or situation be damaging to someone or to some group, or unevenly beneficial to people? Does this decision involve a choice between a good and bad alternative, or perhaps between two "goods" or between two "bads"?

2. Is this issue about more than solely what is legal or what is most efficient? If so, how?

Get the Facts

3. What are the relevant facts of the case? What facts are not known? Can I learn more about the situation? Do I know enough to make a decision?

4. What individuals and groups have an important stake in the outcome? Are the concerns of some of those individuals or groups more important? Why?

5. What are the options for acting? Have all the relevant people and groups been consulted? Have I identified creative options?

Evaluate Alternative Actions

6. Evaluate the options by asking:

   - Which option best respects the rights of all who have a stake? (The Rights Lens)
   - Which option treats people fairly, giving them each what they are due? (The Justice Lens)
   - Which option will produce the most good and do the least harm for as many stakeholders as possible? (The Utilitarian Lens)
   - Which option best serves the community as a whole, not just some members? (The Common Good Lens)
   - Which option leads me to act as the sort of person I want to be? (The Virtue Lens)
   - Which option appropriately takes into account the relationships, concerns, and feelings of all stakeholders? (The Care Ethics Lens)

Choose an Option for Action and Test It

7. After an evaluation using all of these lenses, which option best addresses the situation?

8. If I told someone I respect (or a public audience) which option I have chosen, what would they say?

9. How can my decision be implemented with the greatest care and attention to the concerns of all stakeholders?

Implement Your Decision and Reflect on the Outcome

10. How did my decision turn out, and what have I learned from this specific situation? What (if any) follow-up actions should I take?

This framework for thinking ethically is the product of dialogue and debate at the Markkula Center for Applied Ethics at Santa Clara University.

Primary contributors include Manuel Velasquez, Dennis Moberg, Michael J. Meyer, Thomas Shanks, Margaret R. McLean, David DeCosse, Claire André, Kirk O. Hanson, Irina Raicu, and Jonathan Kwan. It was last revised November 5, 2021.

Thanks and Recognition

The author wishes to thank the Stanley Center for Peace and Security for taking a leadership role in the ethical use of OSINT data. The center is helpful to OSINT analysts across the field, and it has taken an innovative and inclusive approach that helps OSINT attain new levels of professionalism.

The author also extends thanks to the OSINT analysts who were willing to be interviewed for this project, many of whom wish to remain anonymous. From March 15 to April 9, 2021, the author interviewed 25 OSINT experts using video chat.

Seventy-six percent of respondents (19 people) said they faced an ethical dilemma during OSINT research. Only two individuals said they never faced an ethical dilemma; the remainder were not sure. Among the greatest concerns by analysts were ethical issues around privacy and doing harm to bystanders.

Those who managed OSINT analysts occasionally expressed a concern that they were asking employees or volunteers to expose themselves to harmful content during open-source analysis. Violent images and videos, extremist and hate speech, and government propaganda were all cited as examples of "harmful content" by interviewees. Managers were also concerned about their employees' safety and security when using online social media accounts in their own names.

When faced with a dilemma, 64 percent of respondents said they consulted with a peer within their work group, 52 percent consulted with a supervisor or leader, and 44 percent consulted with someone outside their work group. The number one reason for not consulting with someone was the sensitivity of the subject matter.

Five analysts had official written ethical guidance from their workplaces, which were mostly, though not exclusively, universities. The Berkeley Protocol was cited as the most frequently consulted publication on OSINT ethics, and the Stanley Center's Gray Spectrum report came in second. Some analysts cited their background in journalism, law, or philosophy as their main resource for handling ethical dilemmas.

> "Relativity applies to physics, not ethics."
>
> —Albert Einstein

The number one requested resource was additional ethical guidance, followed by voluntary codes of conduct. However, many analysts were concerned that others in the field would not follow the guidance. Several freelancers argued that any form of regulation would disproportionately affect small or solo operators in the field. Some analysts are already preparing for OSINT to become a regular part of legal investigations, for which any open source evidence must meet the standards of courts in their jurisdiction. For example, Bellingcat participated in a mock trial to test evidentiary requirements for court cases. It has cases pending rather may answer whether OSINT can be admissible in court. Less than a third of respondents were interested in joining a guild or association that provided accreditation.

Finally, the author thanks her husband, who is always up to debate ethics or legality—and is often put on the spot to do so. His legal background and good nature made this workbook possible.

About the Author

Melissa Hanham is an independent expert on open source intelligence, incorporating satellite and aerial imagery, and other remote sensing data, large data sets, social media, 3D modeling, and GIS mapping. She is particularly focused on the monitoring and verification of international arms control agreements using open source evidence. She also uses open source information to study export-control systems and proliferation finance activities.

Hanham is an affiliate of Stanford University's Center for International Security and Cooperation and a member of the board of trustees of BASIC in London. She previously worked as the Deputy Director of Open Nuclear Network and Director of the Datayo Project at One Earth Future Foundation in Vienna; at the Middlebury Institute of International Studies in Monterey, California; and at the International Crisis Group in Seoul and Beijing. She holds a BA in International Affairs from the Johns Hopkins University and a master of international affairs from Columbia University's School of International and Public Affairs.

About Us

The Stanley Center for Peace and Security partners with people, organizations, and the greater global community to drive policy progress in three issue areas—mitigating climate change, avoiding the use of nuclear weapons, and preventing mass violence and atrocities. The center was created in 1956 and maintains its independence while developing forums for diverse perspectives and ideas. To learn more about our recent publications and upcoming events, please visit stanleycenter.org.