Objectives

VPNs are security critical applications that people use to bypass geo-blocking, circumvent censorship, and protect their connections from adversaries in repressive environments. Many VPNs in repressive countries have well over 1,000,000 downloads and monthly active users. Their security is dependent on the owners, operators, and developers of these systems yet when the details about who owns, operates, and develops these systems are unavailable, it calls into question the intentions of these parties. The VPN-OSINT Transparency Report Project has three primary goals:

1. Identify the owners, operators, and developers of VPN software used by people in repressive countries to bring transparency to this space

2. Inform users about the degree to which VPN services are operating transparently, and

3. Encourage large organizations like Apple and Google to take the safety of individuals of repressive environments more seriously by clearly identifying VPN applications that operate transparently and those that do not.

The VPN-OSINT Transparency Report will achieve this by collecting and aggregating open source intelligence (OSINT) from disparate sources on the web, synthesizing this information using the Transparency Score, a metric similar to a credit score, and providing details about the transparent and non-transparent organizations in the VPN landscape as well as making recommendations on how organizations can increase their transparency. This scoring methodology is different from simply ranking VPNs from “best” to “worst” because providers that are open about their development, VPNs such as TunnelBear, Lantern, Psiphon, and Mullvad, who appear to operate transparently all score equally high (850), whereas other VPNs such as those listed in Table 1, score low (500). This is desirable as it does not create contentious situations where VPNs have to compete against each other for a single top spot. The preliminary analysis indicates that TunnelBear, Lantern, Psiphon, and Mullvad all score high on transparency and so no contention is created in the community - transparency is rewarded equally.

Data are collected from sites like the Google Play and Apple App store, company websites, WHOIS records, social media sites such as Reddit, Twitter, Telegram, Hackernews, public git repositories, as well as analytical techniques based on automated analysis to compare source code to detect repackaging of applications, and CrypotSluice to analyze transport layer security. Finally, for a selection of applications, manual analysis will be conducted to determine whether the applications have other weaknesses, such as those introduced by third-party libraries, that could undermine user security through data exposure or other issues.

Table 1. Below are a set of VPN apps with tens to hundred of millions of total downloads that are also popular in Indonesia, Russia, India, Pakistan, Saudi Arabia, Brazil, and the UAE. I

found several indicators for each app that they are likely candidates for further consideration and manual analysis. Each of these apps either had no website, a website that is poorly designed or only a few characters long, or the website listed on the Google Play store simply points back to the Play store. Some websites did have links to social media such as Twitter telegram, or Reddit, but the links do not point to anything and few references to these apps exist online. None of the applications appear to have code on Github, gitlab, or gitee suggesting they are not open source.

App Name	Top 3 Most Popular Countries	Developer	# Downloads
Turbo VPN - Secure VPN Proxy	India, Indonesia, Russia	Publisher Country	100M+
Secure VPN－Safer Internet	India, Russia, Turkey	Signal Lab	100M+
SuperVPN Fast VPN Client	Pakistan, India, Saudi Arabia	SuperSoftTech	100M+
WiFi Map®: Find Internet, VPN	Indonesia, India, Brazil	Wifi Map LLC	100M+
HotspotShield VPN: Fast Proxy	US, Saudi Arabia, Turkey	Pango Gmbh	100M+
Normal VPN - Stable&Safe Proxy	India, Pakistan, Mexico	Normal Mobile Tec	10M+
X-VPN - Private Browser VPN	UAE, US,India	Free Connected Limited	10M+

Table 1. Candidate VPN apps popular in highly repressive countries, such as, China, Hong Kong, Taiwan, Myanmar, Vietnam, Pakistan, Saudi Arabia, Egypt, Turkey, Russia, and Kazakhstan, which are mostly considered not free or partly free by FreedomHouse, with download count over 1,000,000 and minimal to no publicly available information about owner, operators, and developers.

Automated data collection will be sourced from websites such as sensortower, Google, ChatGPT, Github, gitlab, gitee, Twitter, Reddit, Hacker News, etc. I will initially rely on US-based web services such as those listed (the exception is gitee which is a Chinese git service) to bootstrap data sourcing and add foreign data sources such as websites as they are discovered.

Data will be collected from websites such as sensortower.com, appfigures.com, Google, Github, gitlab, gitee, Twitter, Reddit, Hacker News, telegram, discord, etc. I will initially rely on US-based web services such as those listed (the exception is gitee which is a Chinese git service) to bootstrap data sourcing and add foreign data sources such as websites as they are discovered.

My current approach is a composite scoring system using the following equation:

Transparency Score = b * B + n * N + d * D + s * S + m * M

The upper case letters represent a numeric value associated with each Transparency Factor and the lower case represent factor weights. The following describes proposed information included in each transparency factor:

1. Business Operations transparency

2. Network Operations Transparency

3. Developer Transparency

4. Social Media Transparency

5. Miscellaneous Information.

(B)usiness Operations Transparency: will consider factors such as whether the VPN has an associated web page, whether there is an “About” page with information about the company’s staff, developers, management team, and other individuals; email addresses, such as whether it appears to be a personal gmail account or a business email address; whether it has a privacy policy; what specific user-information the company collects based on the account creation process and what is stated in the privacy policy, and from where the organization is headquartered. Organizations with a functional website that actually exists, such as Mullvad, Psiphon, Lantern, and TunnelBear have such websites, would score well for Business Operations Transparency, whereas the apps listed in Table 1 by and large do not have functional websites score lower. Organizations that are headquartered from countries with high Reporters without Borders (https://rsf.org/en/index) and Freedom House (https://freedomhouse.org/countries/freedom-world/scores) indices will have higher scores than those with lower scores. An exception I will consider is infrastructure location. Different regions govern PII, data retention, and communications differently. While a provider may be located in a less repressive region, they will likely be required to collect specific information to comply with local laws. I will identify the VPN server locations as stated in their server list. I will factor in how the company handles data and provide details about how their policy differs across infrastructure geographies, which should be provided in the privacy policy or similar documentation.

(N)etwork Operations Transparency: will consider factors such as WHOIS information, whether they use DNSSEC, Registrant Organization in the associated WHOIS record, emails and person of contact. This category is more informational than contributing to the overall score, but in some instances, such as Mullvad, there is additional information suggesting Mullvad operates transparently. Also, many developers either redact information for privacy or the WHOIS records point to a CDN such as CloudFlare. For the five low scoring and five high score apps, more technical information about the transport layer security may be derived from CryptoSluice output which could assess whether the application leaks sensitive client information. Apps with large volumes of invariant content would receive a lower score while those without would score high. Finally, analysis of the servers, such as whether they are susceptible to Port Shadowing or similar attacks as performed in the analysis phase will be included in this Transparency Factor. Apps that are susceptible to such attacks will score low and this would have a high impact on their score whereas lack of such attacks would contribute to a higher score. While the manual analysis portion of the score is more security focused as opposed to business, organizational, or developer transparency, such violations are relevant in the sense that there is an assumption that VPN products protect users and information leaks indicate a lack of transparency.

(D)eveloper Transparency: will consider factors such as whether the app has a git repository, whether the project is open source, what parts of the project are open source, code documentation, and whether they provide security audit information. Projects with a public code repository and that are open source will receive a high score because they have demonstrably transparent development practices, while the lack of them indicates the opposite and hence a lower score. Developer Transparency will factor in client code and configuration, server code and configuration, code comments. Verifying that the code is present and runs as expected is likely a manual process as is reviewing code comments, which developers are notoriously bad at maintaining. The five low scoring and five high scoring apps will additionally include manual and dynamic client analysis such as consistency between the stated privacy policy, information listed in the AndroidManifest.xml file, and how that information is used in the app and transmitted, whether the app is repackaged and/or has compromising additions, and other analyses related to how Android implements its VPN service permission on Linux.

(S)ocial Media & Marketing Transparency: will consider factors such as whether the VPN has a social media footprint (e.g., on Twitter, Reddit, telegram, facebook, instagram, Mastodon, irc, slack, discord and other social platforms), the size of their social network, how they market their product, such as through website ads, social media campaigns, through influencer advertisements, whether they provide localized materials for specific languages, and work with local actors to promote Internet freedom. Applications with at least one social media account will score high in this factor, whereas ones with none will score low. Social media interaction indicates the developer/organization engages with the community which is a sign of transparency. Mullvad, Psiphon, TunnelBear, and Lantern for example have at least a Twitter presence and score high, whereas the apps in Table 1 do not and receive a low score.

Marketing identification will be challenging because specific VPNs may only market to smaller communities or influencers that I may not be able to identify. I will attempt to identify as much marketing during OSINT collection and document how marketing campaigns were discovered and how that channel is being used. Another factor in marketing is whether a VPN provider has a separate website such as a VPN recommendation website. These websites do not appear affiliated with the VPNs they recommend but actually are. This is clearly an attempted manipulation of public opinion and the transparency score would reflect this by being lowered. I will assess the degree to which this can be automated because it is unclear.

I will identify localization attempts by consulting OTF partners that specialize in outreach, identify sources from blogs on the provider website, and if need be, emailing the providers customer support page to determine their practices.

(M)iscellaneous Information: will consider other information that is not directly related to any of the other factors. For example, Mullvad has an onion service and lists a PGP key on their website. This information suggests that Mullvad cares about security and transparency in general.

Members of my support team and I will focus on a technical-heavy and comprehensive report detailing methodologies for data collection, app selection, analysis, scoring. I will use this as the basis for generating non-technical reports used for outreach and advocacy by working with the Usability Lab to tailor the output towards those audiences. I have also attached a mockup report based on preliminary analysis of high and low scoring VPN apps that depicts the envisioned reporting output for non-technical stakeholders. The mockup includes tables that rank VPN apps from high to low transparency scores so that at-a-glance users can assess which apps are more or less transparent. This is followed up with a further breakdown of each VPN's composite score and the scores of each factor individually. This section may also optionally include details about why a particular factor was ranked in a particular way and provide recommendations to address the specific issue. This information will provide recommendations to technical audiences on how to address lack of transparency but can be excluded from reports to non-technical audiences.

Milestones and dates

The following timeline details the proposed tasks and milestones I will perform throughout this engagement.

Background Research Phase

I will generate a list of between 20 and 30 VPN apps that can be downloaded from either Google play or Apple App store in Hong Kong, Taiwan, Myanmar, Vietnam, Pakistan, Saudi Arabia, Egypt, Turkey, and Kazakhstan. Sensortower and AppFigure derive their data from the Google API, and I have tested using the same API endpoints to search specific VPN applications in these same countries. Though these countries will be my focus given their low Freedom House score, I will also factor in additional countries in the global south that also have low Freedom House scores if the specific VPN appears to be used there as well. This list will come from a larger list that I will work with OTF and my supervisor to refine based on the countries in which a specific VPN is popular, whether it has 1,000,000 or more downloads, and any other relevant selection criteria not currently considered. I already have a list of 93 VPNs with information collected using these techniques and have documented my methods used for data collection and analysis for some of these VPN apps.

As stated above, reporting focuses on five key transparency factors: Business Operations Transparency; Network Operations Transparency; Development Operations Transparency; Social Media Transparency, and Miscellaneous Information.

I will collect organization information such as developers, support staff, management team, emails and similar information from the app websites. Other information sources include Twitter, reddit, telegram, discord, github, gitlab, and gitee. Interesting strings, organization names, phone numbers, and email addresses gathered from WHOIS records, company websites, and decompiled APK files can be searched for on social media and code repositories, and this phase of research will assess and possibly include that information depending on how data-rich those sources are.

Month 1: I will enumerate the VPN apps on Google Play and Apple App stores focusing on VPN applications used in countries considered by Freedom House to be “not free” and possibly “partly free”. I will collect ownership, operator, and developer information from their website. I will query WHOIS records and identify holding companies. I will perform analyses to determine other information sources for application owner, operator, and developer provenance. I will document VPN applications that occur on both Android and iOS and download the Android version for static and dynamic reverse engineering. I will begin tool prototyping in this phase. By the end of this month I will have a list of between 20 to 30 VPN apps for consideration and will review the list with OTF to ensure they meet strategic advocacy and outreach goals.

I will consult with OTF to discuss which advocacy groups to meet with. I would like to schedule meetings with advocacy groups in Month 2 to discuss the current VPN app list, the type of analysis we are doing, the reports we intend to generate, and identify gaps between our reporting and what should be generated. This includes identifying language and cultural dimensions that need to be factored into reporting.

I will maintain detailed documentation about sources and methods used for data collection and analysis to be used later in reporting and for future replication.

Month 2: I will continue OSINT collection and analysis in this phase and I will focus on five to six VPNs. I will also perform manual and dynamic analysis of two to three VPNs to establish a static and dynamic analysis workflow. This will assist in identifying tasks that can be automated and those that cannot. This will also help in establishing manual and dynamic analysis methods I will use for later assessments. I will add to my sources and methods documentation to include techniques and tools used. I will refine my methodology and documentation based on requirements identified by the advocacy organizations. I will draft a report and schedule a meeting with the Localization Lab in this phase. I plan to meet with the Localization lab at the start of Month 3 to review the draft report so that it can be refined and so that additional requirements can be identified and issues resolved.

Month 3: I will continue information analysis, site exploration, reconnaissance, and automation requirements specification with another round of five to six VPNs. I will iterate on previously analyzed VPNs if new data sources are identified or for similar reasons. I will also continue manual and static analysis of two VPNs which may be the same or different VPNs from the previous month based on those findings.

I will meet with the Localization lab to review the draft report and discuss requirements for reporting. Depending on the outcome of this meeting, I will schedule a meeting with advocacy organizations to review the Localization lab's refined report version. We will identify needs and adjust my methods and reporting to reflect requirements and issues identified. I will continue to update sources and methods documentation including code and tools developed.

I will work with my supervisor and OTF to identify the appropriate industry standards groups, such as IRTF, its subcommittees, or interested members willing to assist in this effort. I will work to schedule meetings with them at this time. The goal of these meetings is to provide an overview of the project and goals. I will discuss the draft reports we have and any relevant findings. If there are issues that can be resolved through drafting new standards, we will identify directions and schedule additional meetings to discuss in further depth.

Month 4: I should have a good idea about which tasks can and cannot be automated in this phase as well as report structure and format. I will refine the tool's code, processing pipeline, and output format to reflect changes to reporting format and how best to present aggregate results to an analyst for review. For example, all scraped data may be stored in a database and presented via the browser. This could assist in identifying relationships between different VPN applications, developers, operators, or similarities between code libraries used for different VPN applications. I will continue collecting data, adding data sources, and other miscellaneous OSINT tasks that may arise from the previous steps This will focus on a new batch of five to six VPNs and possibly iterating on the previously analyzed VPNs.

I will perform analysis of two to three VPNs in this month using established methods, maintaining documentation, and updating it as necessary. I will schedule a meeting with the Learning Lab in Month 5 to present these results, integrate them into the report we have been working on, and address issues or changes as necessary. I plan to meet with advocacy groups and standards groups in Month 5 to provide updates, identify any changes in requirements or goals, and refine appropriate project elements.

Month 5: I will perform another round of OSINT collection with a new batch of 5 to 6 VPNs. I will continue the manual and dynamic analysis on two to three VPNs in this month as well based on previously established methodology.I will continue documenting sources and methods, and report relevant findings to OTF and affected VPN providers as necessary.

I plan to meet with the advocacy groups to provide updates on findings and identify changes in requirements and goals. I will also meet with the Learning Lab to review results from the previous month to add to the existing report.

Month 6: I should be finishing OSINT data collection for the remaining VPN applications by this month. I will perform additional analysis of two to three VPN applications and document methods and findings as above. I will continue refining the code based on assessments of VPNs I perform this month. I will finish this month with a final list of 5 VPNs with low Transparency scores and 5 with high scores. These 10 VPNs will be the subject of a more comprehensive manual and static analysis assessment for the last six months of this project.

Manual Analysis Phase

In the second six months of this project I will focus more heavily on manual and dynamic analysis based on lessons learned from the previous six months. I will perform a comparative analysis of 5 VPN apps with the lowest Transparency scores and 5 with the highest score. As stated previously, this score is a composite of information related to how transparent the application's business operations, network operations, development operations, social media operations, and miscellaneous security operations are. Preliminary analysis suggests that apps without a website, without a social media presence such as on Twitter, telegram, etc., or broken links to social media sites are, no github and non-open source projects appear to be the least transparent and will serve as a case-studies for deeper manual static and dynamic code and network analysis.

I will perform manual and dynamic analysis on the client APK as well as the server to which they connect. Client-side analysis will consist of tasks such as decompiling APKs to identify what hardware components, such as GPS and location information, device identifiers, contacts, or other information the app is accessing. Many of the VPNs I have already reviewed appear to incorporate third-party advertising libraries in their applications. I will verify this and determine whether the app connects to other services, such as advertisers, and whether they are doing so securely. I will run the apps on a rooted Android device, collecting log information from packet captures and determine how the app stores and transmits information it collects, to what servers that information is sent, and determine who owns those servers. I may additionally leverage the CryptoSluice tool from my previous ICFP engagement to assess whether the applications are leaking private information. It will also be valuable to assess whether these third-party libraries have security issues of their own that could put users at risk. For each VPN, I will document the specific libraries used and review them to determine whether they contain security flaws. All methods used for analysis will be documented. I will review any security related findings with my supervisor and OTF to determine an ethical disclosure plan.

To test the servers, I will perform tests using techniques similar to Port Shadowing that I helped develop to determine whether the servers are susceptible to these types of attacks and also whether another VPN can be tunneled through these provider's servers. Finally, Android implements its VPN permissions by leveraging firewall marks in Netfilter and we suspect the design can lead to the VPN apps being susceptible to attacks such as redirecting client packets to an attacker. I will assess this during manual analysis as it could be a high-impact issue for many Android applications, particularly VPNs. Any findings will be disclosed to OTF for review. We will identify which component is vulnerable, whether it is just the app or the operating system, and notify the appropriate parties. When testing server related issues, I will only send packets and slow rates and only to my own connection to eliminate the possibility that other users are affected by tests I perform.

Month 7: App 1, 2, and 3 analysis. I will apply static and dynamic analysis techniques to the top 1 -3 most inconsistent and incomplete provenance information for this month. This will include running and collecting pcaps, APK code, identifying and analyzing third-party libraries, and testing servers associated with the specific VPN for the app as described above.

I will schedule a meeting with the Learning lab for Month 8 to discuss findings for the manual analysis phase. I will schedule a meeting with the advocacy groups to provide updates on manual analysis findings and determine how these findings can be used. One possibility is working with consumer reports or similar organizations to demonstrate any connection between lack of transparency and poor code security. This could be used by them to encourage Google and Apple to designate specific VPN applications as riskier and/or less transparent.

Month 8: App 4, 5 and 6 analysis. Same as month 7 for a different set of apps. I will add to documentation as appropriate.

Month 9: App 7, 8, and 9 analysis. Same as month 7 and 8 for a different set of top apps. I will add to documentation as appropriate. If it is appropriate, I will schedule meetings with the Learning lab to add to our report. I will also be in regular contact with advocacy and standards groups at this point and will meet as needed.

Analysis & Reporting

Month 10: I will complete manual analysis and testing in this month. I will meet with the Learning lab to provide the remaining findings from manual and dynamic analysis and work with them to add these results to the final reports. I will schedule meetings with advocacy and standards groups for Month 11 and as needed to review results and determine requirements for reporting they might need.

Month 11: I will perform any remaining technical tasks related to tool development, OSINT collection, manual and dynamic analysis. I will focus on cleaning up documentation and research notes. I will meet with advocacy and standards groups as necessary.

Month 12: I will focus on final reporting, cleaning up documentation, and other tasks related to outreach, advocacy, and standards groups requirements. I will also summarize next steps, if any, for this project.

Anticipated outputs and outcomes

My project will produce three primary outputs: An OSINT Collection Tool for automatic data collection and analysis; A Non-technocal Report; and, a Technical Report. Additionally, any vulnerabilities identified during manual analysis will be disclosed and be a secondary output.

OSINT Collection Tool

The tool will be used for automated data collection based on my assessment of which tasks can be effectively automated and repeatable. The envisioned users of this tool are analysts that know how to write, read, and run code. Its purpose is to provide a foundation for future analysts to collect data in a uniform and repeatable way, then place it in a central location for further analysis and reporting. This tool will crawl websites, APIs, WHOIS records, and other sources that can then be reviewed and cross-referenced with other information to learn owner, operator, and developer provenance.

For each VPN app, the tool will generate a credit-like score, the Transparency Score, based on the five components described in the Introduction. Each app will contain a section that highlights the score, and a breakdown of component scores from which the composite score is derived. Each app will also contain a detailed report for each composite score as well as details about why the factor is considered, why it is important for transparency, and how the VPN developer, owners, and operators can improve their score. A positive outcome from this is that it will provide empirical results that advocacy groups can use when informing local populations about which VPNs are safe and which are not. Another is that future analysis will not have to reinvent the wheel or will at least have a starting point from which to base future assessments.

Manual Analysis, Dynamic Analysis, & Vulnerability Reporting

The five most and least transparent apps will include more detailed analysis related to static and dynamic code and network analysis to assess security and highlight potential concerns if they exist or provide information about why that app is secure. I will work with my host organization in reporting the technical findings which could include vulnerability disclosures and reporting. This will include a detailed technical analysis of security issues present and potential impacts to users and will be geared towards industry standards groups composed of developers, engineers, and operators, focusing on specific security issues, if any, identified in the app or server communications. Some variation of this material may also be appropriate to include in the non-technical reporting material that is focused on outreach and advocacy. This will aid them in demonstrating security weakness and emphasize why some VPNs are secure and should be used while others should be avoided. Finally, future researchers doing VPN analysis can leverage the methods and reporting structure from this iteration along with the tool I develop to perform their own analysis and present their findings in a structured and uniform fashion. One positive outcome for manual and dynamic analysis is that if specific VPNs have vulnerabilities, they will be identified and remediated. The impact is two fold. First, security issues will be identified and fixed. Second is that people using the specific VPN will be informed about security weakness and either choose to use a different VPN that is not vulnerable or will at least be well informed about the issues with the VPN they are using.

Non-technical Report

I have created and attached a mockup of the non-technical report I envision delivering. The primary stakeholder for this group are advocacy organizations that work with local populations and assist them in determining which VPNs they should use and which they should not. I will work with the Learning Lab to tailor reporting to assist advocacy organizations in repressive countries when they perform outreach. While this is subject to change based on OTF review, and iterative research during this engagement, I will use this as the basis for developing the finalized reporting materials, and potentially materials in multiple languages based on feedback from advocacy organizations I meet with. The goal of this report is to provide them with empirical results that they can use to demonstrate why some VPNs should be favored and others avoided when working with individuals and organizations. A positive impact from these reports is that they convince users to select VPNs that are less likely to put them at risk of surveillance or other information controls.

Technical Report

The technical report will cover needs and requirements of standards organizations I meet with. This report will provide details on the data collection methodology, sources, and analysis techniques. Each VPN app will have a single score that can be easily interpreted (high score is more transparent and low score is less transparent). It will also contain a summary of the factors from which the overall Transparency score is derived. Finally, Each factor will in turn have its own section providing further details. Text and specific images from sources such as Twitter, company website, screen shots, will go in this section. The final section for each app will cover recommendations for ways to improve transparency and increase the score. I envision two positive outcomes for this report. The first is that a future analyst can use the methodology documented in this report to replicate the analysis for different VPNs. The second is that I can use the report when meeting with standards groups to state specific issues found and how they can be addressed. Having the support of standards organization is more likely to lead to app stores like Google and Apple to take action and designate VPN applications as more or less transparent. This is because Google and Apple likely have affiliations with the standards groups with which I plan to communicate.

In what ways will this effort advance understanding in the relevant field?

There are several organizations working on VPN security. University of Michigan worked with OTF on the VPNalyzer project which focused on testing VPN applications for various privacy and security problems of the tunnel between the VPN client and server. They found several issues where VPN providers leak DNS and IP information or fail to encrypt the traffic even when the VPN has a killswitch feature. Additionally, recent efforts are underway to interview some of the VPN providers. On the other hand, Breakpointing Bad has developed attack techniques against VPN servers that permit an attacker to escalate from off-path to blind in-path, reroute packets to the attacker, infer connections between the VPN server and client, and inject data into a VPN client's VPN tunnel.

Finally, Breakpointing Bad has concurrently submitted an IFF project focused on developing a VPN attack framework that penetration testers can use to execute attacks against different VPN server, client, and operating system configurations similar to Metasploit framework. The attack framework project does not focus on OSINT data collection and is complementary to this effort. The VPN attack framework could be used to perform server assessments and contribute to the Network Operations Transparency score or as part of a completely separate assessment engine focused on security as opposed to provenance and transparency.

My project is complementary to these efforts because none of the other projects focus on determining who owns and operates these VPN services, holding company information for these providers, and whether they are consistent with WHOIS records and other information present online using OSINT. Furthermore, neither have looked at the consistency between implementation and privacy policy or whether the apps are actually developed by the same people/organizations.

Some overlap is present between my analysis of the VPN server and whether attacks can be executed against those servers so that a stealthy adversary can double encapsulate traffic inside an unknowing VPN provider. This overlaps with Breakpointing Bad research, but that research did not look at whether the actual providers were susceptible to any of the attacks they developed, whereas my effort will explicitly develop and test a double encapsulation attack against the providers. Overlap also exists with interviewing VPN providers. My project is complementary to this because unlike interviewing VPN providers directly, which may or may not be possible in some situations, I am focusing on information available through other means that are readily available online and may produce results even when providers are not willing to be interviewed. Finally, this effort is complementary to the VPN attack framework because it focuses on assessing server security and could be used in a separate scoring methodology focused on security rather than transparency and provenance.

What risks or variables could jeopardize the outcomes of the project?

I will be collecting a large volume of data from non-uniform and unstructured web data. This data is inherently messy and requires tedious analyses that can lead to code breakage and slow down development time. I have first hand experience working with this type of data as well as techniques for handling unstructured text data, such as natural language processing, named entity extraction, sentiment analysis, and similar techniques for processing unstructured and semi-structured text data.

Manual analysis is time consuming, however, there are automated techniques based on AndroidManifest file analysis that are used for identifying malware that could be leveraged in concert with my manual analysis and could help reduce analysis time. There are also techniques for determining whether applications are repackaged and/or packaged with bloatware or other potentially compromising software.

How will the applicant protect their safety and security and that of any others involved in the project? (if applicable)

Some of the data collected may include names of people involved in the ownership, operation, and development of the VPNs under consideration. Depending on the specific project, and the views of the team and OTF, I can optionally redact names from reporting and instead include metadata to indicate whether particular roles are available (e.g., has Developer Name, email, etc), though because the project derives its data from open sources that in the the public domain, I do not anticipate redactions being necessary.

Some of the tests I will perform during manual analysis involve sending packets to and through particular servers. I will eliminate disruption of connections that are not my own by only sending packets to my own connections and doing so at rates much lower than normal traffic produced by apps operating under normal conditions, which is relatively high (on the order of thousands of packets per second). Where possible, I may also set up my own VPN server and connect to it if more invasive testing is warranted.

I will run any recommendations made in the report by OTF and my host organization and team members to ensure that I am not, for example, encouraging people to use no VPN at all since this may be even worse than if they were to use a VPN that might be OK by happens to have a low Transparency Score.

What steps will the applicant take to minimize any ethical concerns associated with the proposed project? (if applicable)

As stated in the safety section, some of the data collected may include names of people involved in the ownership, operation, and development of the VPNs under consideration. Depending on the specific project, and the views of the team and OTF, I can optionally redact names from reporting and instead include metadata to indicate whether particular roles are available (e.g., has Developer Name, email, etc).

Again, some of the tests I will perform during manual analysis involve sending packets to and through particular servers. I will eliminate disruption of connections that are not my own by only sending packets to my own connections and doing so at rates much lower than normal traffic produced by apps operating under normal conditions, which is relatively high (on the order of thousands of packets per second). Where possible, I may also set up my own VPN server and connect to it if more invasive testing is warranted.

Finally, any recommendations produced will be run by both my host organization and OTF to ensure messaging does not confuse people into thinking they should never use VPNs.

How is the applicant well equipped to carry out the technical work proposed? (if applicable)

I have experience performing independent research. I am a highly motivated self-starter. I recently completed a 12 month ICFP in collaboration with the University of Michigan. I am still coordinating with them on reporting for that effort, but my technical contributions are quite promising in furthering Internet security as we have identified several issues. The CryptoSluice project also has the potential to factor into this work by analyzing the privacy of a selection of VPN apps. I have experience analyzing software and VPNs. Professor Crandall and I developed several attacks against VPN servers here. That effort was produced using a combination of static and dynamic analysis techniques and testing on both Android, iOS, and Ubuntu Linux that are necessary for this effort.

Additionally, I have working experience working with at-risk populations, developing prototypes that analyze network traffic, testing and auditing application security. I received a three month OTF ICFP fellowship in 2014 and worked at the Citizen Lab where I helped several groups in India manage sensitive infrastructure. That project went on to mature into what is now TibCERT. I performed rapid prototyping of Zeek IDS scripts and python code to generate Zeek code during a summer fellowship at the International Computer Science Institute. There, I used Zeek to identify network traffic at Lawrence Berkeley Laboratory and compare HTTPS headers to Tor HTTPS headers to identify fingerprintable information.

Finally, I worked as a penetration tester and automation developer and team lead for three years at a New Mexico startup called RiskSense. There, I performed penetration tests using Nessus, Nexpose, and OpenVAS to perform vulnerability scans and Metasploit for vulnerability exploitation. I also contributed to an in-house penetration testing tool that automated much of this work by executing OpenVAS and nmap scans, running common exploits against vulnerable systems, then moving laterally for further exploitation. Finally, I proposed and led the prototyping, development and implementation of a similar system that collected and synthesized open source intelligence of CVE's used in exploitation and applied machine learning techniques to rank the vulnerabilities based on how likely they were to be used in real attacks.