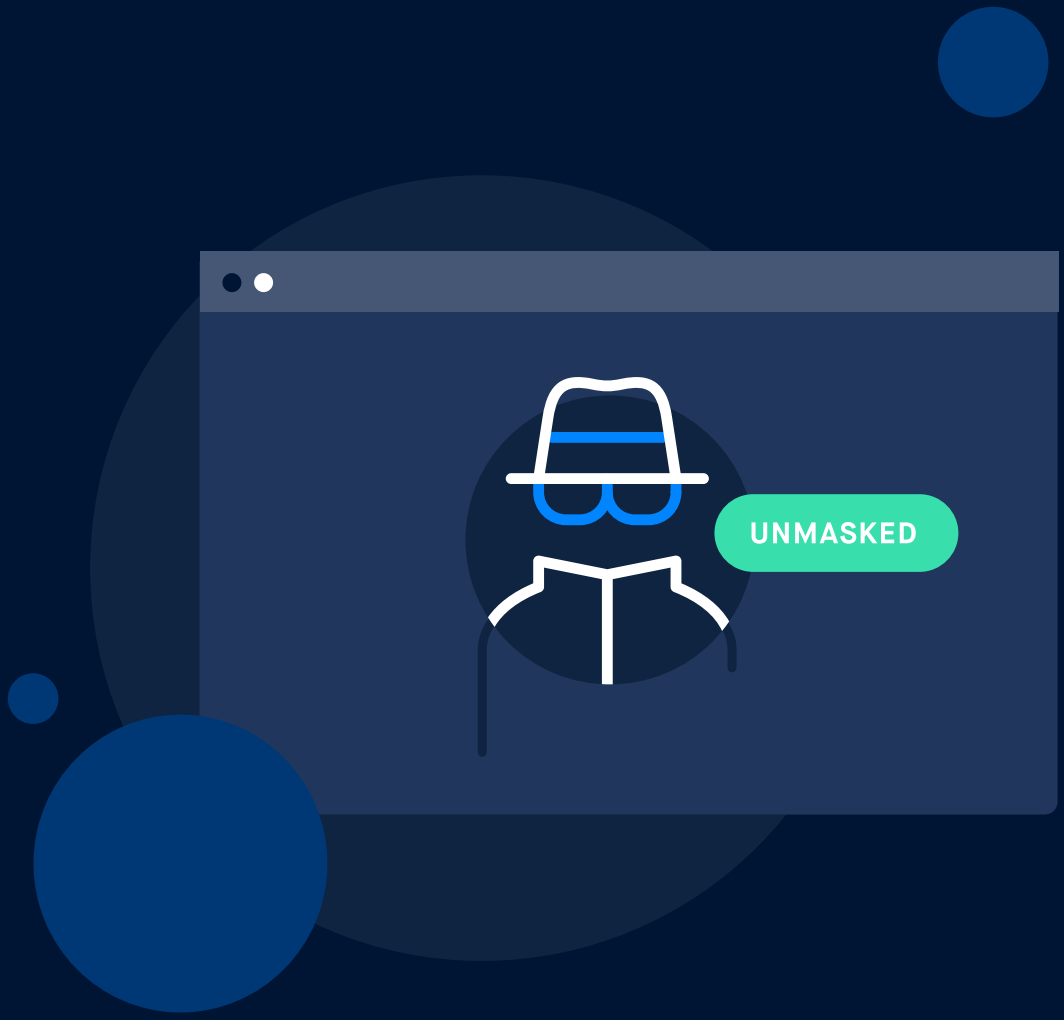
Anonymization – A Threat to Children Online

Unmasking Online Predators With VPN and Proxy Detection



GEOCOMPLY

IMPACT

Introduction

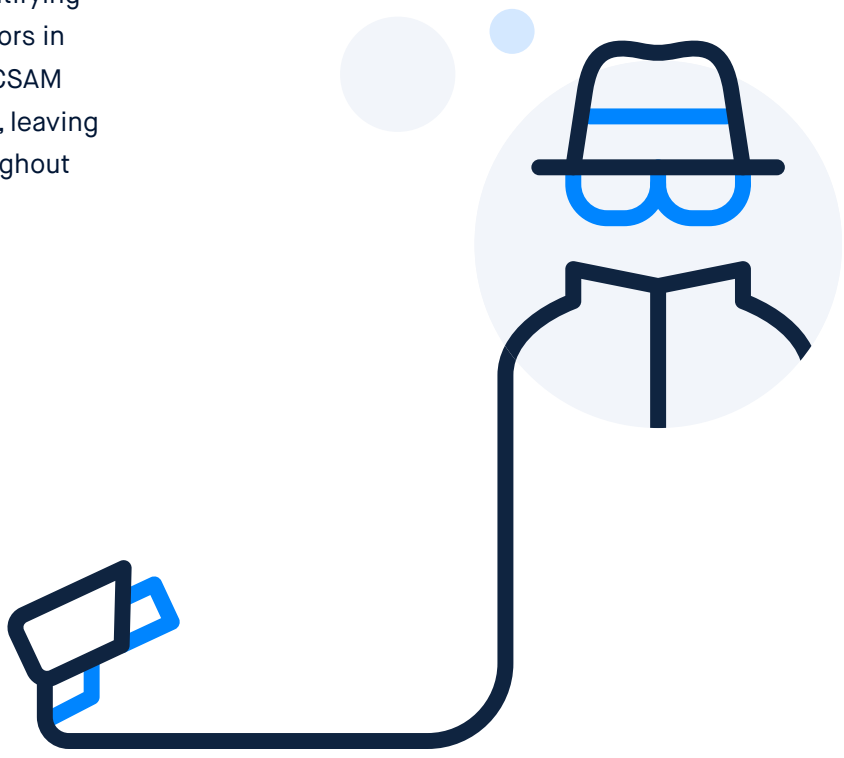
The internet has broken down barriers to inclusion, connected societies, spurred innovation and enhanced efficiency. However, it has also created new opportunities for criminals to conduct illegal activity and exploit people online.

Children are particularly vulnerable to the dark realities of the internet. Predators exploit children by taking advantage of loopholes in the same identity verification and anonymizing tools we use daily. Online child sexual exploitation (OCSE) and the funding, production and distribution of Child Sexual Abuse Material (CSAM) have been exacerbated by the ability to anonymously share data on the internet.

With images and videos easily copied and shared on many online platforms, CSAM spreads faster than it can be taken down. Darknets, encryption services, anonymization technologies, and peer-to-peer file-sharing services have created a safe harbor for offenders. Consequently, law enforcement faces many obstacles in identifying and prosecuting criminals, trapping survivors in a cycle of continued victimization. Often, CSAM resurfaces well after the abuse has ended, leaving victims feeling unsafe and exploited throughout their lives.

To combat OCSE, nonprofits, technology providers, law enforcement, and families must come together. Information sharing, collaboration and technology are central to the fight against child exploitation.

The following paper focuses on one technical solution for child safety that enhances the data available to law enforcement for investigations and creates avenues for collaboration between organizations fighting CSAM. By taking practical steps to uncover masked actors, we can make the internet a safer place for everyone.



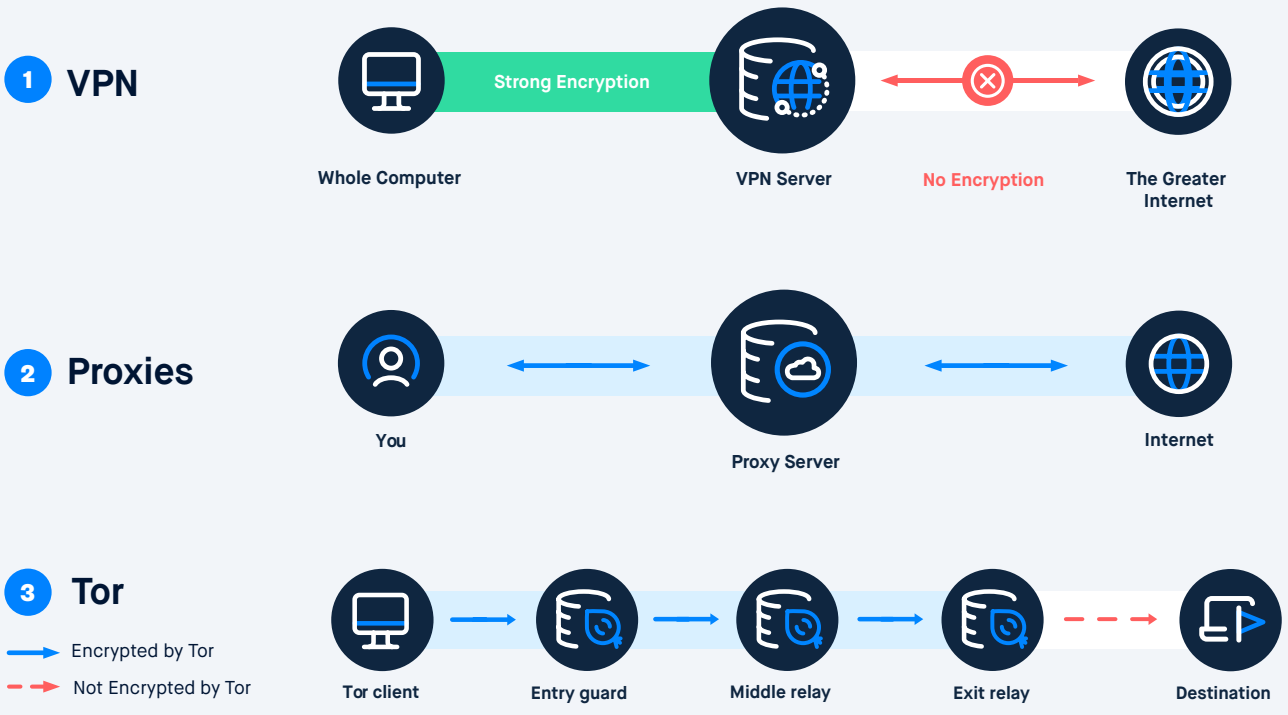
The Explosion of Anonymity

Nowadays, high value is placed on user privacy, and people have various motivations to operate anonymously online, such as accessing geofenced streaming content, evading censorship or bypassing firewalls.

On a daily basis, millions of people around the world use anonymizing tools, such as virtual private networks (VPNs) and proxies. Researchers have found that 1 in 3 internet users have a VPN. These numbers are higher in certain countries such as the United States (U.S.), where nearly half of users claim to use some type of VPN.

Anonymizing tools can conceal a user's real internet protocol (IP) address, which is unique to each device and can reveal one's general location. Commonly used anonymizing tools include:

1. **VPNs:** VPNs encrypt internet traffic and redirect it through a specially configured remote server run by a VPN host.
2. **Proxies:** Proxies do not encrypt internet traffic; rather, they send it to a Proxy, then forward it to the Internet, acting as the source of the request.
3. **Tor:** The Tor network (Tor is short for The Onion Router) routes traffic through various nodes, wrapping it in encryption each time. A computer that uses a Tor browser never communicates directly with the website's server.



VPN and proxy providers use sophisticated techniques to evade detection. For example, certain providers deliver "residential proxies" as a service to their customers. Residential proxies are innocent users' home IP addresses that have been hijacked through various techniques by internet service providers (ISPs) and re-sold as a premium anonymizing service. The residential IP hijacking tactic avoids using data centers that VPNs and proxies have traditionally relied on, making it even more difficult to detect.

The most common uses of VPNs include accessing geofenced streaming video content. IP addresses have long been the standard way streaming video companies like Netflix and Hulu determine what content users may watch, depending on their location and respective copyright contracts.

VPNs help users access geographically restricted content by allowing their IP addresses to appear to be located in permitted regions.

However, the ability to anonymously operate online is also appealing for much darker purposes, including the distribution of child sexual abuse material (CSAM). Criminals can easily manipulate anonymizing tools to evade oversight and conduct illicit activity online.

> "Criminals use various countermeasures to ensure their operational security online, and rely in so doing on services such as virtual private networks (VPNs), proxies and anonymous or The Onion Router (TOR) browsers."
>
> – Europol, 2021

Masking Illegal Activity

VPNs and other internet anonymizers enable the funding, production and circulation of CSAM. The Virtual Global Taskforce has found that some of the largest threats in online child sexual exploitation and transnational child sex offending are the increased support for personal privacy and anonymization technologies. The WeProtect Global Alliance affirms that even offenders with minimal technical knowledge can obfuscate law enforcement investigations by using anonymizers such as Tor and VPNs.

These trends are exhibited in Suspicious Activity Reports (SAR) filed to regulators. The Financial Crimes Enforcement Network (FinCEN) recorded a 147% increase in OCSE-related SAR filings between 2017 and 2020, observing that OCSE offenders are increasingly using convertible virtual currency, peer-to-peer mobile applications, the darknet, and anonymization and encryption services to try to avoid detection.

The ability to anonymously share data online threatens law enforcement's ability to conduct investigations and places extreme pressures on organizations dealing with cyber tips by obfuscating the data available to identify offenders. Worst of all, it traps a child in a cycle of direct and indirect victimization.

Case Study:

- In 2020, international law enforcement agencies shut down a VPN service that had enabled hundreds of thousands of illegal online transactions involving images of child abuse and other illicit activity.
- An OSCE offender based in China exploited children via peer-to-peer file sharing sites, often using a VPN to hide his IP address.
- A U.S. Federal Bureau of Intelligence (FBI) investigation found that a cyberstalker used various anonymizing services, including Tor, VPN services, anonymized international texting services and offshore private email providers to conduct their predatory activity.

> "More offenders are using anonymizing technologies such as TOR as well as VPNs to commit sexual offences against children online."
>
> – The Virtual Global Taskforce, 2019.

The Scale of the Problem

Nonprofits and law enforcement are fighting OCSE on a daily basis. Child exploitation reports to the National Center for Missing & Exploited Children (NCMEC) increased by 28% between 2019 and 2020, with reports totalling 21.7 million in 2020. That is nearly 60,000 reports every day.

With more youth spending time online, there are more opportunities for exploitation. The Canadian Centre for Child Protection (CCCP) saw an 88% increase in reports during the COVID-19 pandemic. Girls appear in the overwhelming majority of CSAM, making up 80.42% of children depicted in the material assessed by the CCCP.

CSAM appears on a variety of online platforms and services, including websites, email, instant messaging, peer-to-peer networks, internet gaming sites, social networking sites, and anonymized networks. This makes the tasks of removing CSAM and identifying offenders hugely complex.

Organizations fighting OSCE require all the tools, insights and information they can obtain to unmask criminals and protect children.

1 in 3 luring attempts reported to cybertip.ca happened on Instagram, Snapchat or KIK messenger.

SOLUTION: Industry-Leading VPN and Proxy Detection

GEOGUARD

VPN and proxy detection tools serve a critical role in the fight against the manipulation of anonymizing tools by criminals. While there is a host of products available in the market, a number of nonprofits and law enforcement agencies have turned to GeoComply's industry-leading products for help.

GeoComply's award-winning VPN and proxy detection solution, GeoGuard, provides multi-layered protection against malicious spoofing tools and techniques. GeoGuard dynamically tracks and flags compromised VPNs, proxies, Tor exit nodes, residential proxies and other types of IP address manipulation. GeoGuard is a database of IP addresses compromised by anonymization services been independently tested to detect IP fraud with 99.6% accuracy. Using advanced and proprietary techniques combined with human intelligence, GeoGuard is continuously updated with new IPs multiple times per day, as well as expiring old IPs to ensure fewer "false positives."

Available as a locally hosted database or via API, GeoGuard is a simple solution to combat even the most advanced IP spoofing methods. By cross-referencing IP addresses associated with OSCE offenders, GeoGuard streamlines investigations, provides insights into IP addresses commonly used by offenders, and empowers investigators with enhanced analysis.

Key Features

Fraudulent IP address database

Provides a dynamic, continuously updated list of IP addresses identified as fraudulent.

Device-agnostic

A customizable spoof-proof geolocation solution that works with a wide range of devices and user interfaces.

Predict emerging threats

Leverages GeoGuard's machine learning and human intelligence, to predict and counter emerging threats.

Real-time rules engine

Recognize methods of deception used to mask the true nature of fraudulent IP addresses.

Advanced location spoofing

Detects advanced location spoofing techniques such as proxy over VPN and residential IP hijacking.

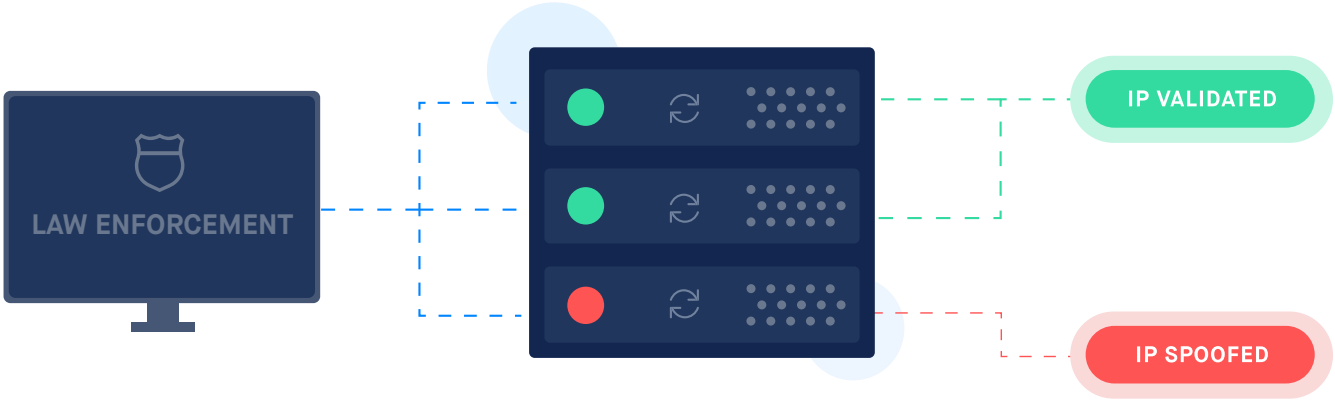
Industry-verified

Approved and recommended to help uncover anonymous bad actors.

Case Study:

The Child Rescue Coalition uses GeoGuard to analyze IP addresses relating to OSCE offenders. GeoGuard provides actionable evidence in law enforcement investigations relating to the distribution of CSAM. The Child Rescue Coalition states:

> "The utility of the GeoComply assistance to our mission is already proving itself. It is crucial that we're able to provide the most accurate information possible to our law enforcement users. It is not an exaggeration to say that GeoComply will literally help stop and, in some cases, even prevent the sexual abuse of a child."
>
> – Glen Pounder, Chief Operating Officer, Child Rescue Coalition



Looking Ahead

Productive steps can be taken to protect existing and future generations from online predators. Legislators, regulators, industry, nonprofits and law enforcement have an opportunity to leverage technical solutions, share information and collaborate to make the internet a safer place for everyone.

Technology, while not the sole solution, is a core component of the path towards a safer internet. VPN and proxy detection is one meaningful step forward in this area. Cryptocurrency exchanges, video-sharing platforms, social media sites and other online platforms only need to take small steps, such as implementing VPN and proxy detection, to have an impact on the investigation and prevention of OSCE.

With greater data intelligence, online platforms are able to help regulators and law enforcement better identify suspicious activity. As a result, online environments are made safer, more offenders can be taken off the streets, and children can enjoy the benefits of the internet without the risk of exploitation.

GeoComply welcomes partners to join us in taking a stance for a safer internet. To learn more about how GeoComply can help protect children and support investigations, contact our IMPACT team: impact@geocomply.com

About GeoComply

Founded in 2011, GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. GeoComply is dedicated to harnessing our resources to protect children, support law enforcement and enhance internet safety. Through collaboration with nonprofit, public and private sector partners, we fight online child exploitation.

The company's software is installed on over 400 million devices worldwide and analyzes over 4 billion transactions a year, placing GeoComply in a unique position to identify and counter both current and newly emerging fraud threats.

Proven and refined over 10 years of development, GeoComply's solutions incorporate location, device and identity intelligence along with advanced machine learning to detect and flag fraudulent activity. By integrating GeoComply's solutions into their processes and risk engines, organizations are able to identify fraud earlier in a user's engagement, better establish their true digital identity and empower digital trust.

GEOCOMPLY IMPACT

To learn more about how GeoComply can help protect children and support investigations, contact our IMPACT team:

impact@geocomply.com