GeoComply

December 14, 2023

Executive Manager
Industry Regulation and Legal Services
Office of the eSafety Commissioner
PO Box Q500
Queen Victoria Building
NSW 1230
Via email: submissions@esafety.gov.au

Dear Commissioner,

RE: Office of the eSafety Commissioner Consultation on the Draft Online Safety Industry Standards 2024

On behalf of GeoComply Solutions, thank you for the opportunity to engage with the Office of the eSafety Commissioner to discuss children's online safety. Founded in 2011, GeoComply provides fraud prevention and cybersecurity solutions that detect location fraud and help verify a user's true digital identity. We deliver compliance-grade, end-to-end geolocation and user authentication solutions. Our award-winning products are based on the technologies developed for the highly regulated and complex online gaming (iGaming) and sports betting market. Beyond iGaming, GeoComply provides geolocation fraud detection solutions for streaming video broadcasters and the online banking, payments, and cryptocurrency industries, building an impressive list of global customers, including Amazon Prime Video, BBC, Akamai, Sightline, DraftKings, FanDuel, and MGM.

Our software is installed in over 400 million devices worldwide and analyzes over ten 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 ten years of development, GeoComply provides the industry's most accurate location detection solutions, combining multi-source data collection and verification through machine learning and human intelligence. By integrating GeoComply's solutions into their processes and risk engines, organizations can identify fraud earlier in a user's engagement, better establish their true digital identity, and empower digital trust.

Supporting law enforcement and protecting children from digital exploitation via technology is central to our mission. GeoComply's corporate social responsibility division, IMPACT, focuses on fighting online child sexual exploitation (OCSE) through technology by partnering with nonprofits and law enforcement and collaborating with the private sector through channels such as WeProtect Global Alliance. We have been longstanding partners with the National Center for Missing and

545 Robson St #5
Vancouver, BC V6B 1A6
Canada

GeoComply.com
solutions@GeoComply.com
+1 888 822 9339

Exploited Children (NCMEC) and the Child Rescue Coalition (CRC), as well as other global nonprofits fighting OCSE and supporting investigators.

By way of this letter, GeoComply addresses Question 7 outlined in the Discussion Paper on the Draft Online Safety Industry Standard 2024. Namely, examples of systems, processes and technologies that can disrupt and deter the use of a relevant electronic service to solicit, generate, distribute or access child sexual abuse material (CSAM) and pro-terror material, which should be highlighted in the guidance.

OCSE is an issue that is unfortunately enabled by the ability to operate and share data on the internet anonymously. Online offenders can easily circumvent the existing identity verification protocols on online platforms, facilitating and perpetuating online harm. Our comments focus on technical tools that strengthen identity protocols to help disrupt and deter the use of a relevant electronic service to solicit, generate, distribute or access CSAM and pro-terror material.

1. Background

The proliferation of the internet and digital technology has led to an increased risk of child sexual exploitation and abuse online. Data from NCMEC shows that reports of child sexual exploitation have increased in recent years, with a 28% increase in 2020 alone[1]. Additionally, research from the Canadian Centre for Child Protection (C3P) shows that a significant portion of CSAM depicts children under the age of twelve, with girls being disproportionately represented[2]. Moreover, despite reporting offending accounts, victims have been known to be revictimized due to offenders' accounts either remaining active or the offender gaining access to the victim through separate accounts when the initial account was blocked, deleted, or removed by the platform operators[3]. This issue, called device recidivism, leads to offenders being able to re-victimize children online and find new victims on platforms even when they have already been banned or removed by the platform.

Online criminals tend to spoof or falsify identity and device data to operate anonymously online and evade oversight. Many social media companies report the volume of fake accounts they are actioning on their platforms. For example, in Q3 2023, Meta actioned 837 million fake accounts[4]. Falsifying identifying information when establishing an account is mainstream and can be facilitated through anonymization tools. An estimated 1.6 billion people use Virtual Private Networks (VPNs) globally[5], which encrypt internet traffic and redirect it through a specifically configured remote

[1] National Center for Missing and Exploited Children (2023). Link: https://www.missingkids.org/gethelpnow/cybertipline
[2] Canadian Centre for Child Protection (2021). Link: https://annualreport2020.iwf.org.uk/trends
[3]Canadian Centre for Child Protection (2022). Link: https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[4] Meta (2023). Link: https://transparency.fb.com/reports/community-standards-enforcement/fake-accounts/facebook/
[5]Surfshark (2023). Link: https://surfshark.com/blog/vpn-users

server run by a VPN host. Such anonymization tools are used for legitimate purposes, such as evading censorship or for security[6]. However, anonymization tools are also readily available to bad actors who wish to circumvent identity protocols and establish fake accounts to conduct illicit activity online anonymously, such as sharing CSAM or other illicit content. In the absence of concrete, quality data relating to a user's profile, device, related accounts, or (as needed) identity information, social media platforms face tremendous obstacles in disrupting bad actors from conducting their illicit activity on their platforms. Moreover, law enforcement and regulators face barriers to investigating online criminal activity.

Based on our experience operating in the geolocation and fraud detection space for over ten years, we know that cybercriminals may leverage various forms of location-altering technologies to hide their location and, therefore, their identity, allowing them to conduct illicit activities anonymously. Location obfuscation tools include (but are not limited to) Remote Desktops, Proxy Servers, TOR (The Onion Router) exit nodes, emulators, and jailbroken or rooted devices. Darknets, encryption services, and peer-to-peer (P2P) file-sharing services have created a safe harbor for offenders[7]. This is affirmed by the Virtual Global Taskforce[8]:

> *'More offenders are using anonymizing technologies such as TOR as well as VPNs to commit sexual offences against children online.'*

Offenders' ability to circumvent identity protocols on online platforms and set up fake accounts poses a threat to the safety and well-being of children. On the topic of the financial sextortion of children, C3P found that:

> *'Extorters can seemingly create multiple accounts that appear legitimate through careful curation or by hacking/taking over an existing account and repurposing it for their use. We believe extorters may also purchase stolen or hacked accounts from online communities dedicated to cybercrime. Victims have remarked that extorters often recycle the likeness of a profile, using the same images and name construction to operate multiple accounts simultaneously.'*[9]

Subsequently, strengthening identity verification protocols and the mechanisms used to prevent account recidivism is critically important to disrupt and deter the use of electronic services to solicit, generate, distribute or access CSAM and pro-terror material.

---

[6] Surfshark (2023). Link: https://surfshark.com/blog/vpn-users

[7] Police Foundation (2017). Link: https://www.police-foundation.org.uk/2017/wp-content/uploads/2022/07/turning_the_tide_FINAL-.pdf

[8] Virtual Global Taskforce (2019): http://virtualglobaltaskforce.com/wp-content/uploads/2020/02/2019-Virtual-Global-Taskforce-Environmental-Scan_Unclassi.pdf

[9] Canadian Centre for Child Protection (2022). Link: https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

2. **Systems, processes and technologies that can disrupt and deter the use of a relevant electronic service to solicit, generate, distribute or access CSAM and pro-terror material**

To combat issues relating to the establishment of false or anonymous accounts and prevent malicious actors from perpetuating harm online, GeoComply recommends leveraging device fingerprinting and authenticated multi-source geolocation data (GPS, Wi-Fi Triangulation, cellular, etc.) as part of onboarding and authentication processes. Collecting actionable and dynamic data both strengthen platforms' ability to:

- Prevent bad actors from re-entering online platforms;
- Stop the proliferation of fake accounts;
- Strengthen record-keeping capabilities, and
- Enhance the ability to identify criminals.

Harms can be addressed by readily available technology that utilizes multiple data sources to verify users, whether to locate predators or intercept fraudsters in real time. As a non-biased, privacy-preserving strategy to ensure internet safety and strengthen Know Your Customer (KYC) processes, multi-source geolocation, device data, and anonymizer detection are critical parts of child exploitation investigations and increasingly vital tools for fraud detection. These data points enhance a user's risk profile without compromising their natural identity. Markets that embrace multi-source geolocation data and the detection of anonymizers in their KYC processes (such as regulated online gaming in the U.S.) have demonstrated that online safety can be achieved while preserving privacy.

Steps available to mitigate the risk of victimization from anonymous accounts include:

- Identifying suspicious location patterns relating to online criminal behaviour by leveraging multi-sourced geolocation data for anti-fraud purposes;
- Leveraging multi-sourced geolocation insights and device fingerprint technology to prevent offenders from revictimizing victims or repeatedly circumventing device and account-level bans;
- Empowering platforms with greater actionable insights by integrating multi-source geolocation and anomalous behavior detection into their existing risk management frameworks to protect children and better enforce platform terms of service;
- Keeping records regarding risk management framework for harm reduction, enforcing terms of service, and preventing device recidivism.

Conclusion

Given the alarming statistics on child exploitation and online fraud, it is imperative that we take immediate action to address the issue of anonymization and its impact on internet safety. GeoComply outlines the tools that are exploited by online criminals to share, upload and distribute harmful online content anonymously, and the reasonable steps available to meet certain

GeoComply

expectations. We hope that by sharing our insights based on our experience operating in the geolocation and fraud detection space, we can collectively make the internet a safer place for all consumers. GeoComply offers these comments to assist the eSafety Commissioner in its mission to safeguard our children.

Thank you for your commitment to preventing online harm. We would welcome the opportunity to discuss these matters with the Commissioner at the earliest convenience.

Yours sincerely,

Anna Sainsbury

Anna Sainsbury
President, Executive Chairman and CEO
[redacted]

545 Robson St #5
Vancouver, BC V6B 1A6
Canada

GeoComply.com
solutions@GeoComply.com
+1 888 822 9339