GEOCOMPLY

11/3/2021

Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
GPO Box 2154
Canberra ACT 2601
Via email: OnlineSafety@infrastructure.gov.au

Dear Director,

RE: Draft Online Safety (Basic Online Safety Expectations) Determination 2021

On behalf of GeoComply Solutions, thank you for the opportunity to engage with the Department of Infrastructure, Transport, Regional Development and Communications, to discuss matters relating to online safety.

GeoComply delivers digital identity, geolocation and fraud detection solutions to diverse industries. Supporting law enforcement and protecting children from digital exploitation via technology is central to our mission.

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

By way of this letter, GeoComply addresses the following expectations set forth in the Draft Online Safety (Basic Online Safety Expectations) Determination 2021:

- The provider will take reasonable steps regarding anonymous accounts;
- The provider will take reasonable steps to prevent access by children to class 2 material;
- The provider will keep records regarding certain matters.

GeoComply outlines the tools that are exploited by online criminals to anonymously share, upload and distribute harmful online content, and the reasonable steps available to meet certain 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.

I. Expectation: The provider will take reasonable steps regarding anonymous accounts

GeoComply applauds the expectation that the provider will take reasonable steps regarding anonymous accounts. Online child sexual exploitation (OCSE) is an issue that is unfortunately enabled by the ability to anonymously share data on the internet. One of the first layers of protection a bad actor will utilise to mask their true identity is a tool to spoof their internet protocol (IP) address, such as a proxy service, a virtual private network (VPN), Tor, or another type of anonymiser.

The WeProtect Global Alliance affirms this point, stating the following:

> *'Even offenders with minimal technical knowhow can complicate the detection of crimes by using anonymisation solutions such as Tor and Virtual Private Networks (VPNs), which are now mainstream and built into some browsers by default. The overall effect is a significant hindrance to investigations caused by technologies with a low barrier to use.'* [1]

Therefore, when dealing with OCSE offenders, IP addresses are only useful when cross-referenced against a database of known anonymisers. Fortunately, technology exists that can support organisations investigating criminals who exploit anonymisation techniques.

II. Reasonable steps available to meet the expectation regarding anonymous accounts:

Geolocation and fraud detection solutions help to uncover anonymous actors and mitigate illicit activity. Therefore, reasonable steps available to meet the expectation regarding anonymous accounts include:

- Leveraging IP spoofing detection to investigate offenders;
- Identifying location-based typologies relating to online criminal behaviour by leveraging multi-sourced geolocation data in age and identity verification.

For example, the Child Rescue Coalition (CRC) leverages GeoComply's IP fraud detection capabilities to assist with OCSE investigations. GeoComply provides the CRC with

[1] WeProtect Global Alliance, Global Threat Assessment 2021 (2021), page 27: https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=/wp-content/uploads/Global-Threat-Assessment-2021.pdf&dButton=true&pButton=true&oButton=false&sButton=true#zoom=0&pagemode=none

multi-layered fraud protection against VPNs, proxies, peer-to-peer networks, and other types of data manipulation, which is utilised in their analysis of the data relating to child sexual abuse material (CSAM), to provide actionable intelligence to law enforcement.

With enhanced intelligence around location data and anonymising technologies, organisations dealing with OCSE offenders are better-placed to uncover and help prosecute anonymous criminals.

III. Expectation: The provider will take reasonable steps to prevent access by children to class 2 material

The expectation placed on the provider to take reasonable steps to prevent access by children to class 2 material is an important one.

In a recent British Broadcasting Corporation (BBC) investigation[2], ineffectual age and identity systems for the OnlyFans platform have led to the circulation and consumption of CSAM on the platform. The investigation found that under-18s have used fake identification to set up accounts, with one fourteen-year-old using their grandmother's passport.

In line with the Draft Online Safety (Basic Online Safety Expectations) Determination 2021, service providers must leverage technical (or other) measures to prevent access by children to certain material and/or platforms.

IV. Reasonable steps available to meet the expectation regarding preventing access by children:

There are a range of age verification methods and solutions to meet the expectation of preventing access by children. For example:

- Verifying date of birth according to existing data, such as on an ID or credit card
- Cross referencing the ID with a selfie which users must upload to prove they are the owner of the ID

The effectiveness of such solutions in preventing access by children diverges significantly from other procedures, such as simply requesting a prospective user to provide their date of birth. Such simple steps are ineffective in preventing underage access and fail to meet policy expectations. Therefore, distinguishing between certain age verification methods is important to highlight.

[2] BBC, Noel Titheradge and Rianna Croxford, The Children Selling Explicit Videos on OnlyFans (May 27, 2021): https://www.bbc.co.uk/news/uk-57255983

V. Expectation: The provider will keep records regarding certain matters

A core barrier to investigating online criminals and predators is frequently the lack of identity information collected on and/or disclosed by certain platforms. Moreover, online criminals tend to spoof or falsify identity data to evade oversight.

Platform record-keeping and the associated issues with online safety are highlighted by recent allegations[3] around Pornhub (owned by MindGeek) that relate to the hosting of CSAM and non-consensual content.

Before the Canadian Ethics Committee, MindGeek made the following statement:

> *'MindGeek preserves data related to all identified and reported CSAM incidents to permit law enforcement investigation. This includes the content itself, the user's details, and, where available, the* ***IP addresses*** *associated with the user's access to our platforms.'* [4]

A method to spoof an IP address is usually the first tool in a bad actor's arsenal before conducting some nefarious activity online, including the sharing of CSAM or other illicit content.

In the absence of concrete, quality identity data relating to a user's profile, law enforcement and regulators face huge obstacles to investigating online criminal activity, such as hosting and circulating CSAM.

VI. Reasonable steps available to meet the expectation regarding record-keeping

Reasonable steps can be taken to ensure that valuable and actionable data is available to law enforcement and regulators to assist with investigations.

Easily falsified and manipulated data points, such as IP addresses, fail to meet expectations regarding record-keeping. Service providers should take steps to enhance their identity verification protocols, and where possible, verify the authenticity of the data collected.

For example, due to the criminal exploitation of IP address anonymisers, IP addresses are only useful when cross-referenced against a database of known anonymisers. Moreover, multi-source geolocation data (GPS, WiFi Triangulation, cellular, etc.) gives far more accurate

[3] NY Times, Nicholas Kristof, The Children of Pornhub (December 4, 2020): https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html

[4] MindGeek, ETHI - Invitation to Appear (February 1, 2021), page 6: https://www.ourcommons.ca/Content/Committee/432/ETHI/Brief/BR11079307/br-external/MindGeek-e.pdf

insights into a user's location than an IP address and strengthens Know Your Customer (KYC)/onboarding protocols.

Collecting such valuable and dynamic data as part of an onboarding process strengthens a platform's record-keeping capabilities; enhances its ability to create a secure digital identity for its consumers, and more readily enables the identification criminals.

VII. Final Remarks

GeoComply offers these comments to assist the Department in its mission to safeguard persons online. Thank you for your commitment to preventing online harm and please don't hesitate to schedule a meeting to discuss these matters in further detail.

Yours sincerely,

[redacted]

Anna Sainsbury
President and Chairman
[redacted]