

From: Vytautas Paukštys [REDACTED]
Subject: Re: Citizen Lab Report
Date: October 14, 2026 at 10:29 AM
To: Ronald Deibert [REDACTED]
[REDACTED]



Dear Ron,

Thank you for the opportunity to comment. Sharing our feedback on your report.

Eskimi has clear rules and controls designed to detect and stop advertisers who try to misuse our platform. Campaigns and creative tags are screened by independent third-party ad-verification vendors as well as by our own monitoring tools.

In this case, the advertiser's tags were built to evade automated scanning. They loaded different code depending on who was viewing the ad, including the device, IP address and location, and campaigns were often restricted to very narrow IP target lists. This is how they passed third-party verification. Our own monitoring flagged this behaviour, and campaigns and individual tags were stopped as our controls detected them. We have since shared the relevant technical indicators with our supply partners.

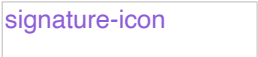
In the interest of supporting your research, the indicators we identified include creative tags calling remote "getAd" loaders hosted on [dtech.adtimizer.co](#), several [mtrtb.com](#) subdomains (noas, infinoas and ppv2), and [events.myweb3id.io](#). Because these loaders served different code depending on the viewer and targeting, they were not detected by third-party ad-verification scanning. Additional technical information can be provided where it is useful for your research.

Discover-Tech had been a self-service advertiser on the Eskimi DSP since 2022, under our standard advertiser terms. Because of our campaign and individual tag blocks, its activity remained small, amounting to only a few hundred dollars in media spend. Its last campaign through the Eskimi DSP was stopped on 6 August 2026, and no impressions have been served since. Once the full pattern of the advertiser's behaviour became clear, we permanently blocked all of its accounts, users and associated domains.

We are working with independent ad-security specialists to help identify similar behaviour across the industry.

As I mentioned, happy to contribute with anything that can help with further investigation and ensuring compliance in the ad-tech market.

Kind regards,
Vytas



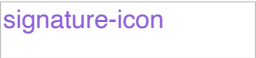
Vytas Paukstys
CEO/Founder
[REDACTED]
[REDACTED]
[REDACTED]

On Wed, Oct 14, 2026 at 3:54 PM Vytautas Paukštys [REDACTED] wrote:
Hello Ronald,

Thank you for your quick response. I will send our official response within the next hour or so.

The main reason I reached out, though, was to offer some additional pieces of the puzzle for your research. As a DSP, we have some technical data on our side that may be useful, such as how the campaigns were targeted. Given how sensitive that data is, I thought a short call first would help us agree on what's useful and whether and how we can share it properly.

I won't be able to do a call today, but tomorrow works for me. Just let me know if you think it would be useful. Either way, our official response will follow shortly.



Vytas Paukstys
CEO/Founder
[REDACTED]
[REDACTED]
[REDACTED]

On Wed, Oct 14, 2026 at 3:35 PM Ronald Deibert [REDACTED] wrote:
Dear Vytautas Paukštys:

Thank you for reaching out. We sought comment from a number of companies that will be mentioned in the report. Your response alerted us to the fact that we intended to send Eskimi a request for comment but it inadvertently never left our outbox. We apologize for this

oversight.

As you know, we are publishing a report on Discover-Tech Ltd. We found that Discover-Tech Ltd. facilitates the delivery of mercenary spyware via targeted advertisements. Our research establishes that Discover-Tech operates a platform called Controlium that enables multiple mercenary spyware partners to de-anonymize, fingerprint, and automatically infect devices the moment an advertisement is rendered. We found that Discover-Tech Ltd. delivers both malicious and benign ads via several advertising vendors including Google, Yandex, FreeWheel, Eskimi, Liftoff, and Sunteng. We also found that Discover-Tech Ltd. works closely with mercenary hacking company Candiru.

Our report includes the following findings regarding Eskimi:

The source code of Discover-Tech Ltd.'s campaign management system indicates that Discover-Tech Ltd. used Eskimi as one of three DSPs for ad delivery. URL telemetry data reviewed by us confirms the delivery of Discover-Tech Ltd. ads via Eskimi DSP, based on parameters in requests to Discover-Tech Ltd.'s impression logging that referred to Eskimi.

If you can provide us with a comment before 5pm ET today, we can include this response in the report (alternatively, we can include the email above as your response).

If we do not receive a response from Eskimi before 5pm ET today, we will update our published report with any response you send after that time.

Sincerely,

Ronald Deibert, O.C., O.Ont
Director, the Citizen Lab, Professor, Political Science
Munk School of Global Affairs & Public Policy
University of Toronto
<https://citizenlab.ca/>
<https://deibert.citizenlab.ca/>