Ghost Protocol – Snapchat as a Method of Surveillance

By:
Richard Matthews, Kieren Lovell and Matthew Sorell

From the proceedings of
The Digital Forensic Research Conference
DFRWS EU 2021
March 29 - April 1, 2021


THE UNIVERSITY of ADELAIDE
TAL TECH
DFRWS 2021
VIRTUAL EUROPE
Snapchat as a method of Surveillance
GHOST PROTOCOL

THE UNIVERSITY of ADELAIDE

TAL TECH

Authors

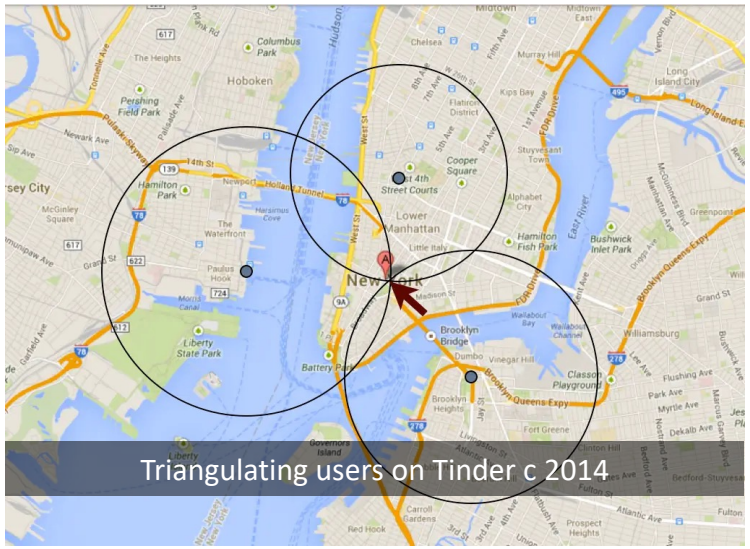
- Dr Richard Matthews
- LCDR Kieren Lovell
- Dr Matthew Sorell

Research questions

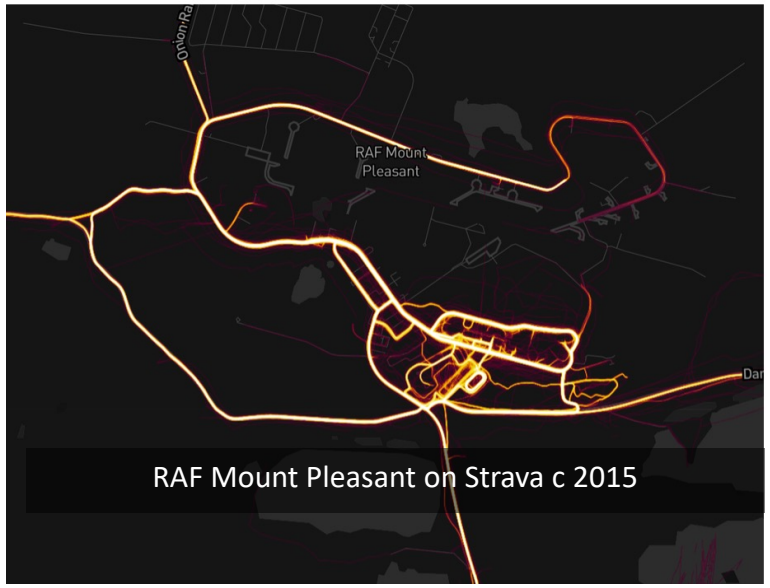
For forensic purposes:

- Can Snapchat be used as a distributed surveillance system?
- How do we easily extract media from Snapchat?
- Can we verify this media for surveillance purposes?

Previous work



Triangulating users on Tinder c 2014



RAF Mount Pleasant on Strava c 2015

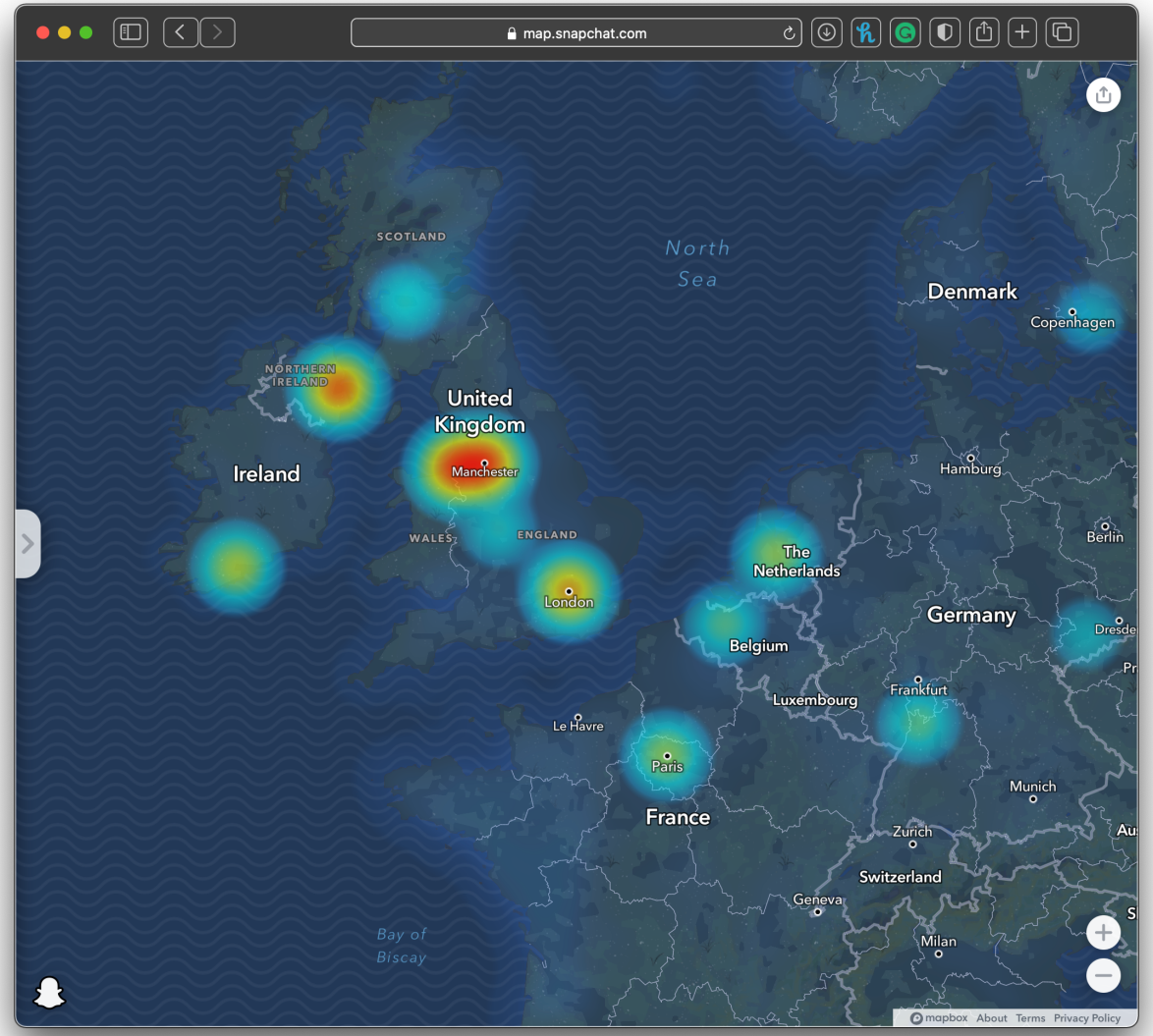

Tracking military vessels using Snapchat c 2018

Surveillance system characteristics

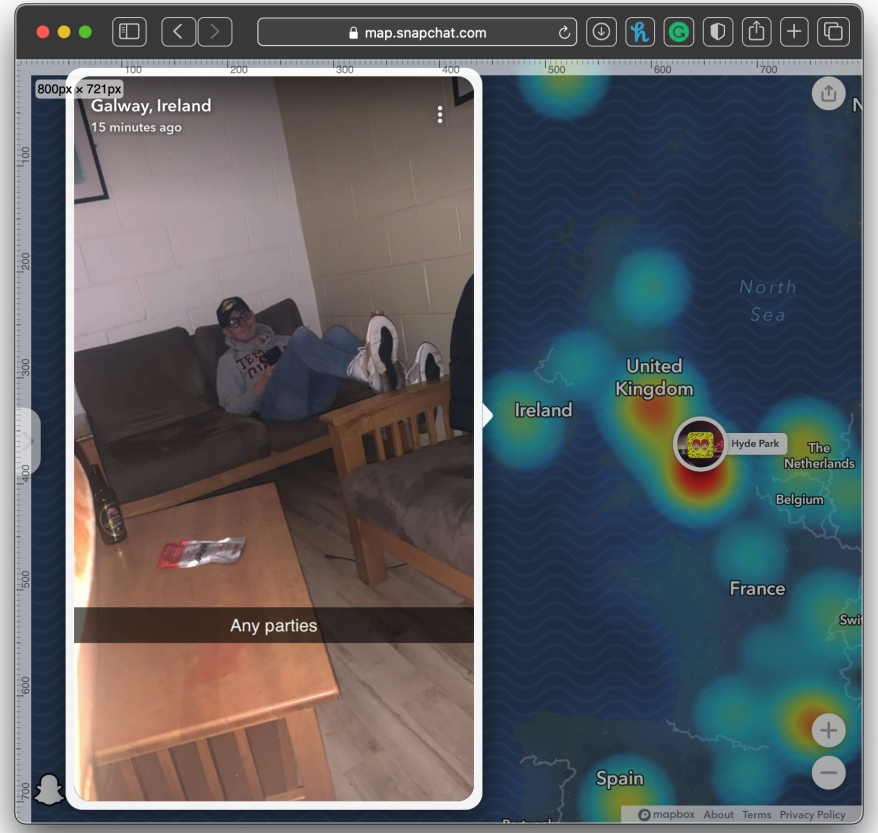
1. Identify facial features at entry, exit and transaction points
2. Read license plates
3. Recognize clothing worn by persons of interest
4. Monitor general activity in areas accessed by public
5. Ability to track people through a site
6. Sufficient frame rate to track movement
7. Easily extracted while respecting privacy without coercion or spoliation

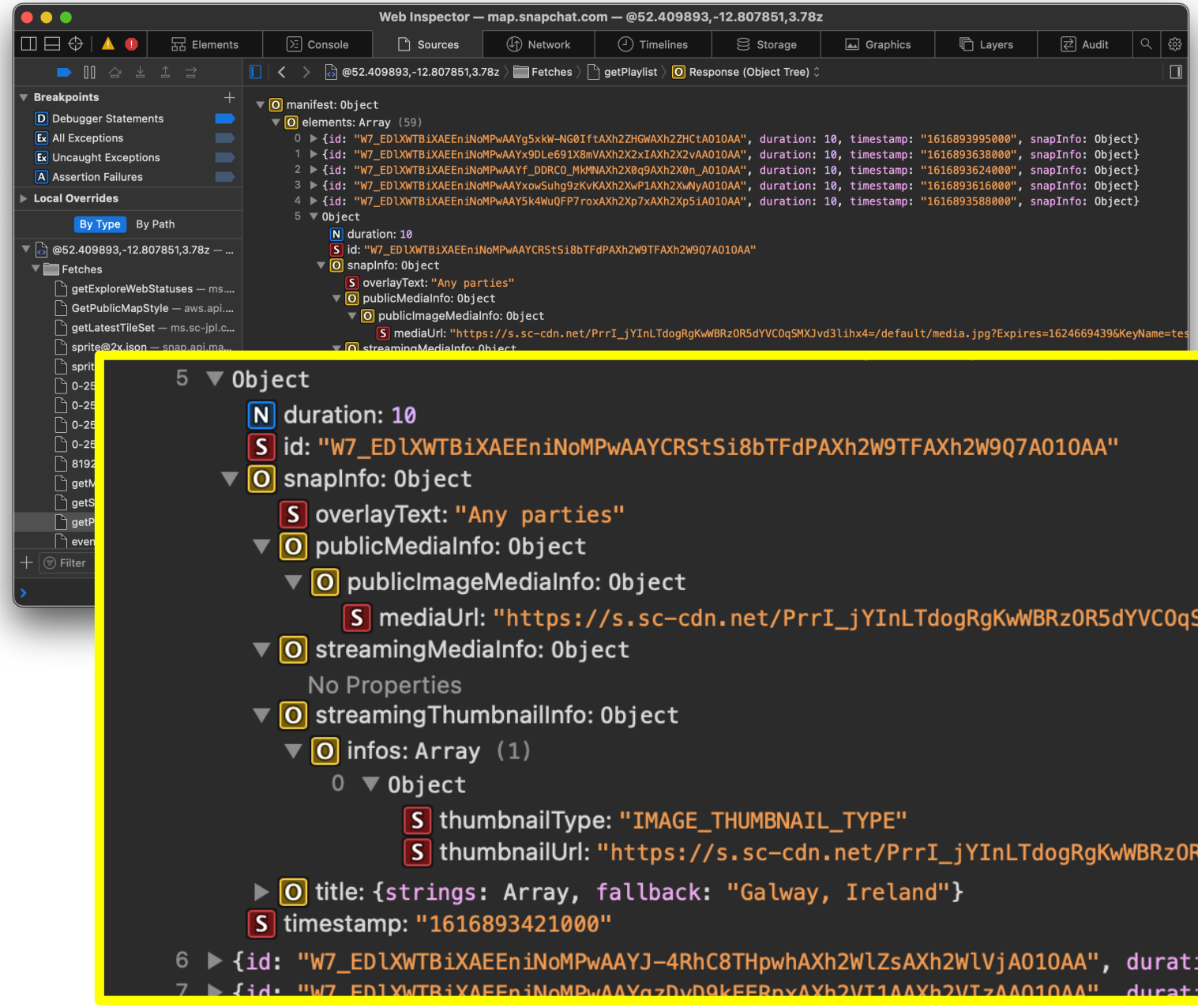
Extraction

Extraction


map.snapchat.com
SCOTLAND
North Sea
Denmark
Copenhagen
NORTHERN IRELAND
United Kingdom
Manchester
Ireland
Hamburg
WALES
ENGLAND
Berlin
The Netherlands
London
Germany
Belgium
Luxembourg
Frankfurt
Le Havre
Paris
Munich
France
Zurich
Switzerland
Geneva
Bay of Biscay
Milan
mapbox About Terms Privacy Policy

Extraction


map.snapchat.com
800px × 721px
Galway, Ireland
15 minutes ago
Any parties
North Sea
United Kingdom
Ireland
Hyde Park
The Netherlands
Belgium
France
Spain
mapbox About Terms Privacy Policy


Web Inspector — map.snapchat.com — @52.409893,-12.807851,3.78z
Elements
Console
Sources
Network
Timelines
Storage
Graphics
Layers
Audit
Breakpoints
Debugger Statements
All Exceptions
Uncaught Exceptions
Assertion Failures
Local Overrides
By Type
By Path
Fetches
getExploreWebStatuses — ms....
GetPublicMapStyle — aws.api....
getLatestTileSet — ms.sc-jpl.c...
Filter
@52.409893,-12.807851,3.78z
Fetches
getPlaylist
Response (Object Tree)
manifest: Object
elements: Array (59)
duration: 10
id: "W7_EDlXWTBiXAEEniNoMPwAAYCRStSi8bTFdPAXh2W9TFAXh2W9Q7AO1OAA"
snapInfo: Object
overlayText: "Any parties"
publicMediaInfo: Object
publicImageMediaInfo: Object
mediaUrl: "https://s.sc-cdn.net/PrrI_jYInLTdogRgKwWBRzOR5dYVCOqSMXJvd3lihx4=/default/media.jpg?Expires=1624669439&KeyName=tes
No Properties
streamingThumbnailInfo: Object
infos: Array (1)
thumbnailType: "IMAGE_THUMBNAIL_TYPE"
thumbnailUrl: "https://s.sc-cdn.net/PrrI_jYInLTdogRgKwWBRzOR5d
title: {strings: Array, fallback: "Galway, Ireland"}
timestamp: "1616893421000"
{id: "W7_EDlXWTBiXAEEniNoMPwAAYJ-4RhC8THpwhAXh2WlZsAXh2WlVjAO1OAA", duration

Dr Richard Matthews (drrichar...

132 Reputation - Rank

41

#867521 CreatorID leaked from public content posted to SnapMaps

Share:

State: Resolved (Closed)

Disclosed: December 19, 2020 9:18am +1030

Reported to: Snapchat

Reported at: May 7, 2020 10:38am +0930

Asset: app.snapchat.com (Domain)

CVE ID:

Weakness: None

Bounty: $1,000

Severity: Medium (4 ~ 6.9)

Participants:

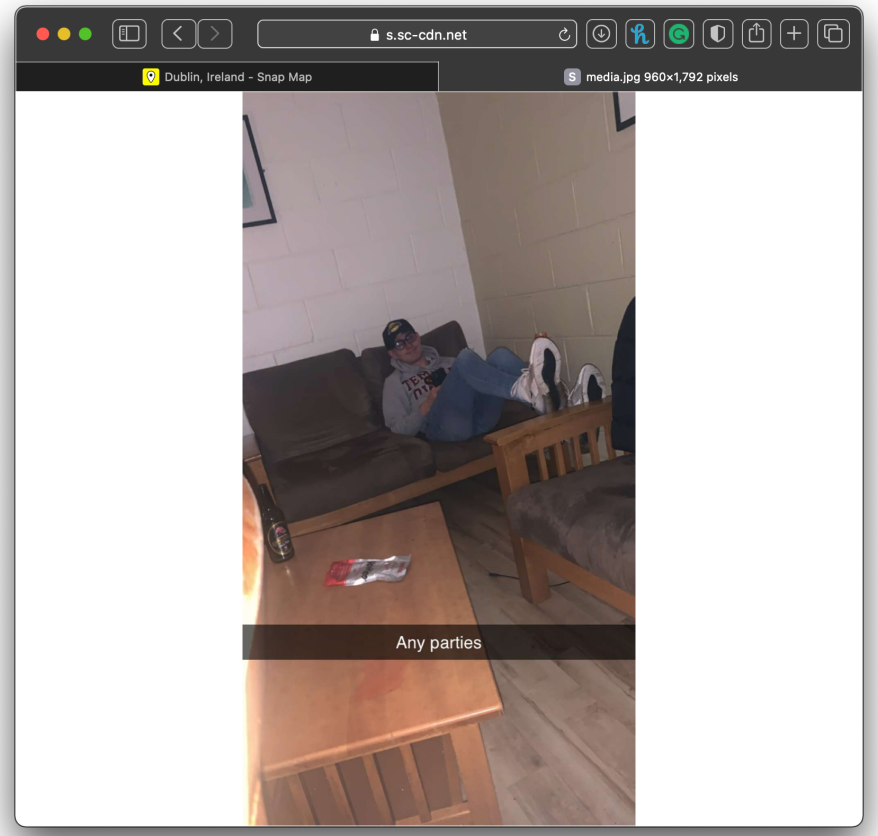
Visibility: Disclosed (Limited)

Collapse

SUMMARY BY SNAPCHAT

TL;DR - the Snap Map media responses unnecessarily return a creatorId. The creator's Snap username cannot be immediately derived from creatorId, but users can use the creatorId to correlate multiple public snaps with that creator. The impact is limited by the fact that all Our Story Snaps that appear on the map go through manual curation, ensuring that most selfie Snaps are filtered out.

Extraction – content and metadata

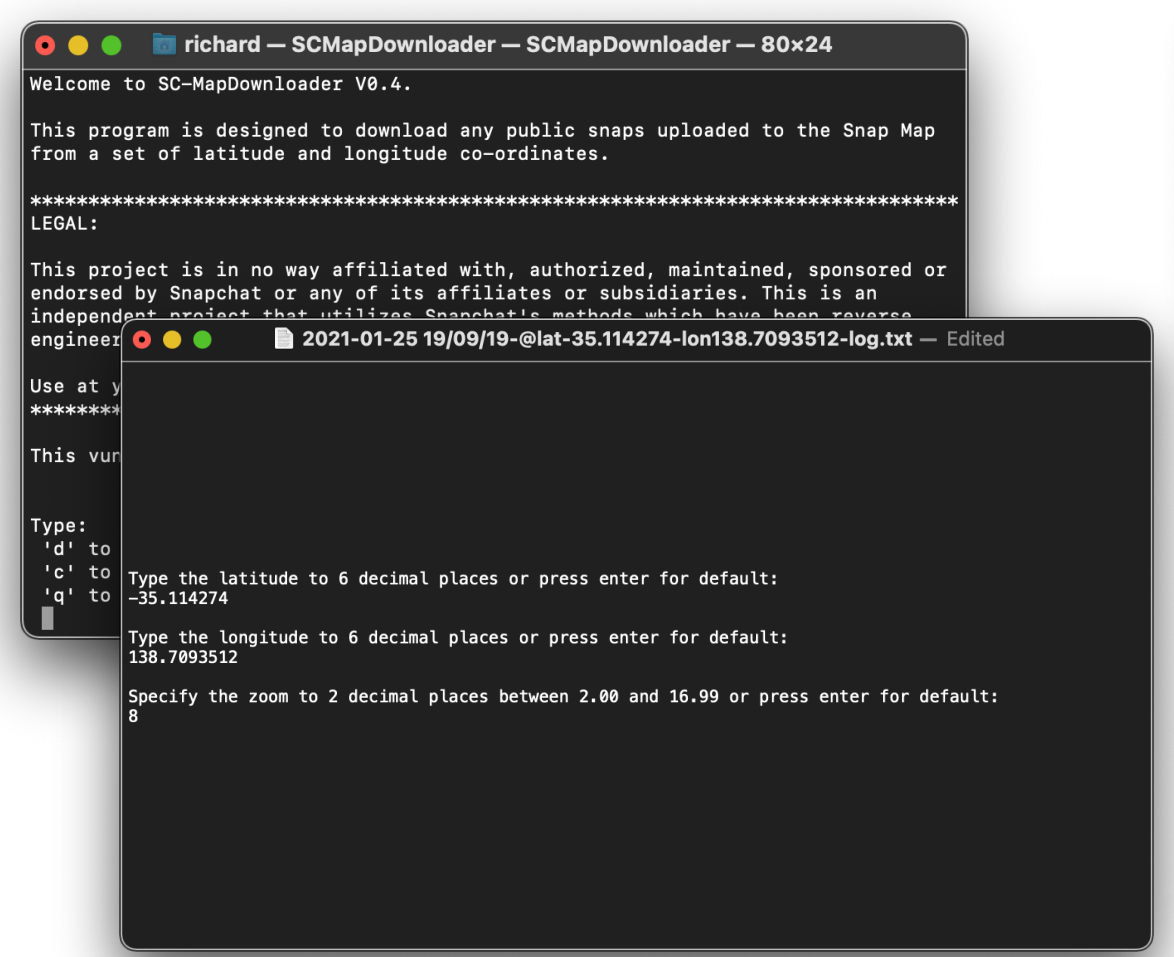


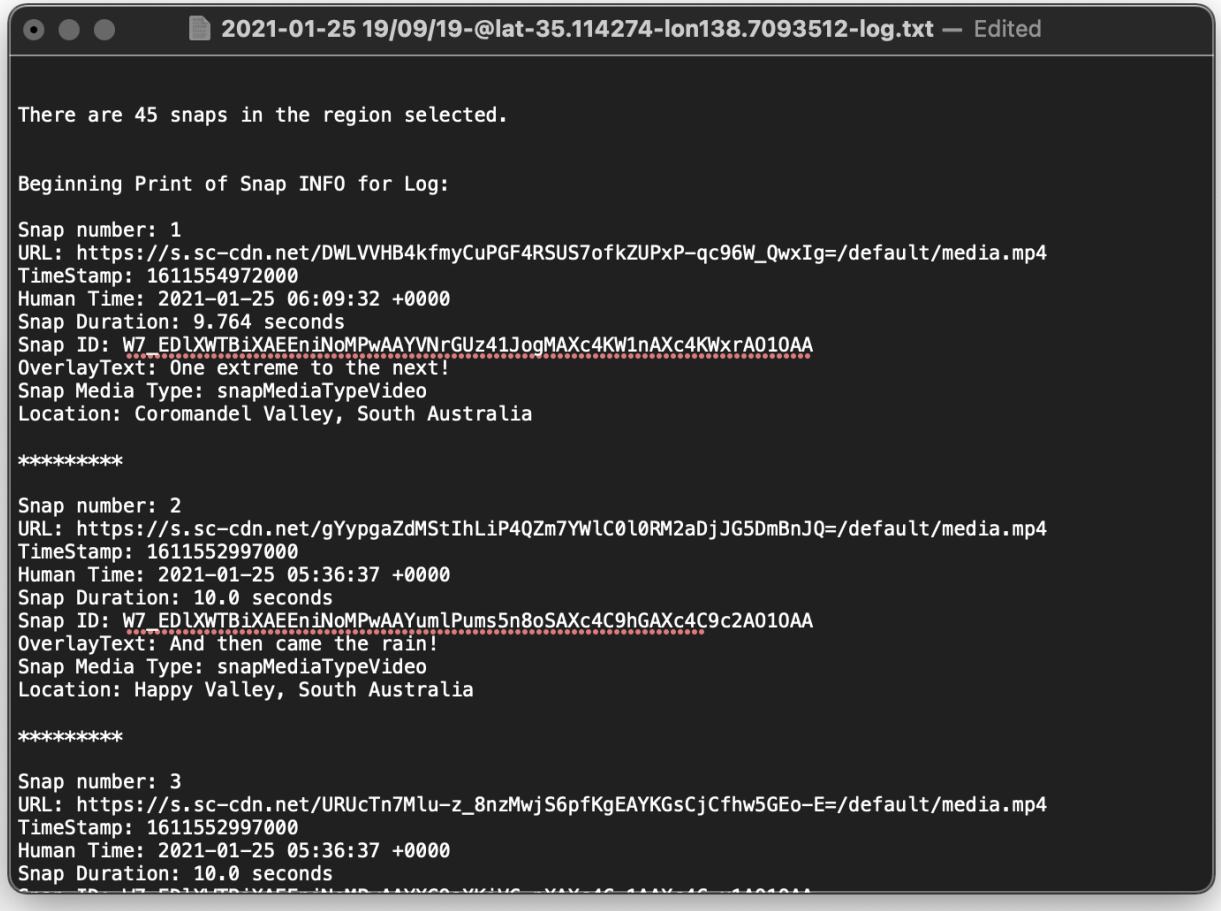

```
5 ▼ Object
    N duration: 10
    S id: "W7_EDlXWTBiXAEEniNoMPwAAYCRStSi8bTFdPAXh2W9TFAXh2W9Q7AO1OAA"
  ▼ O snapInfo: Object
      S overlayText: "Any parties"
    ▼ O publicMediaInfo: Object
      ▼ O publicImageMediaInfo: Object
          S mediaUrl: "https://s.sc-cdn.net/PrrI_jYInLTdogRgKwWBRzOR5dYVCOqSMXJvd3lihx4=/default/media.jpg?Expires=1624669439&KeyName=tes
    ▼ O streamingMediaInfo: Object
        No Properties
```

```
        S thumbnailUrl: "https://s.sc-cdn.net/PrrI_jYInLT
      ▶ O title: {strings: Array, fallback: "Galway, Ireland"}
        S timestamp: "1616893421000"
6   ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYJ-4RhC8THpwhAXh2WlZsAXh2WlVjAC
```

Since publishing this work Snapchat has started sanitizing the URLs of images only to redact part of the "Signature". Work around is to just exclude everything after the "?"

Extraction - Automated



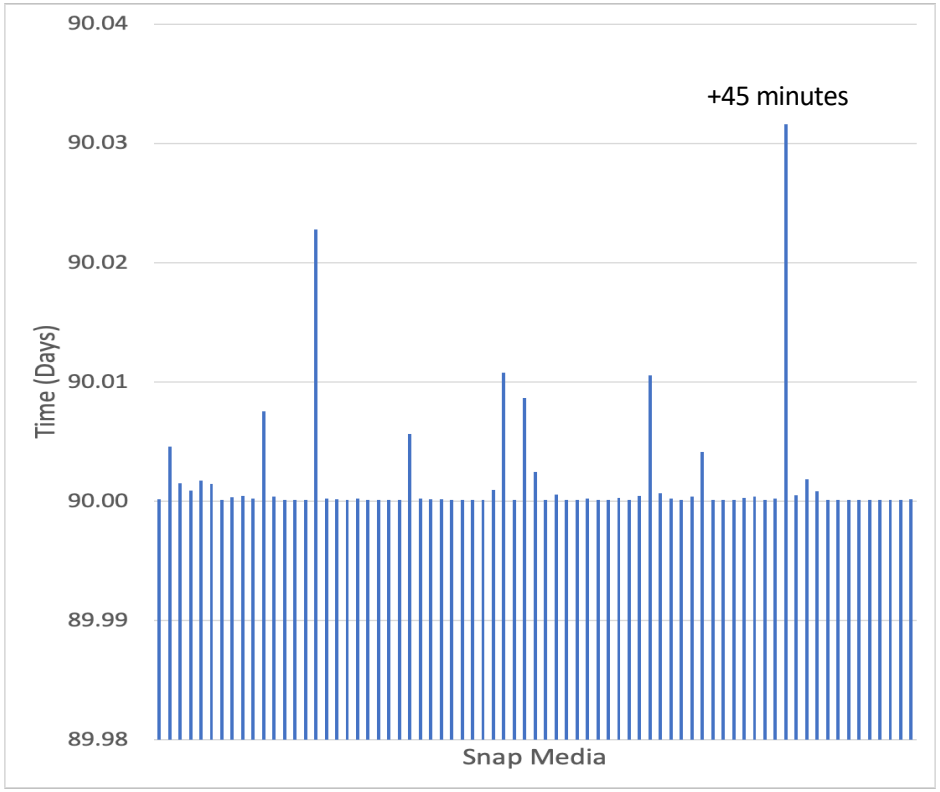


Availability - Ephemeral, Perishable, Transient

Table 3: Snapchat Deletion Policy

Snap Item	Deletion Time
After viewed by all recipients	Immediately
Unopened Snaps	30 days
Your Story	24 hours
Custom Story	24 Hours
Our Story or public stories	24 - 48 hours +
Location data from Map	40 Days

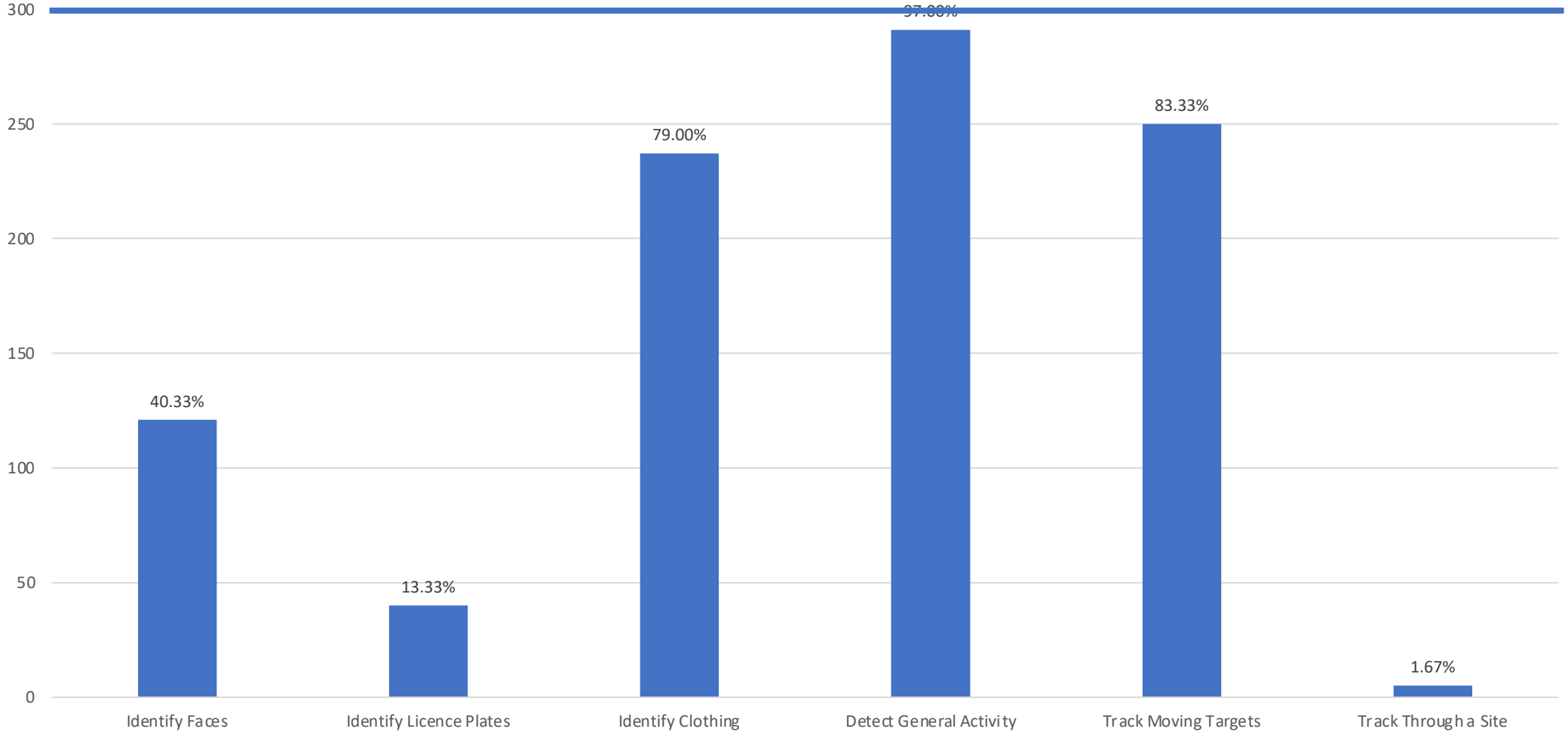
KEY RESULT

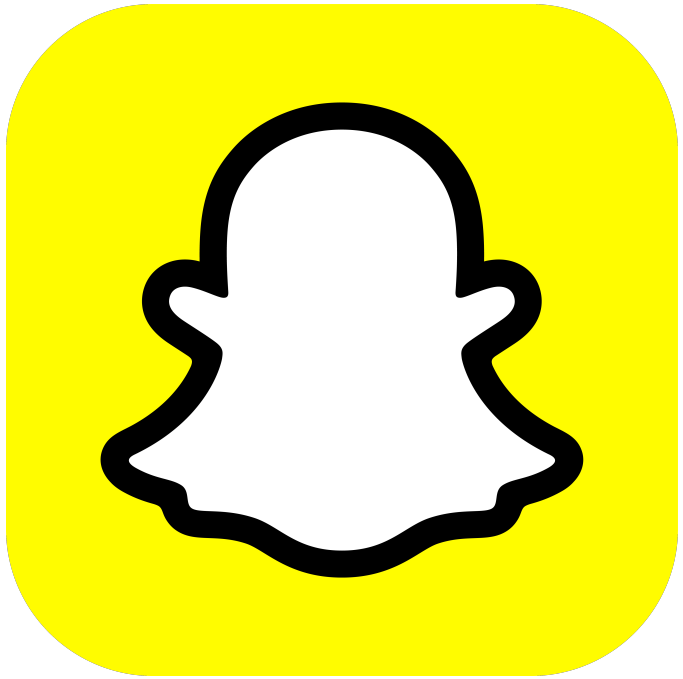


We can add:

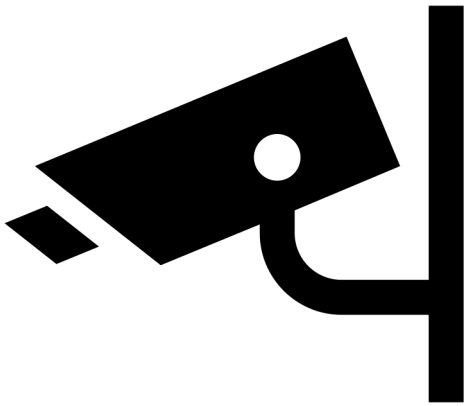
Access on servers 90 days

Validation


300
250
200
150
100
50
0
40.33%
13.33%
79.00%
97.00%
83.33%
1.67%
Identify Faces
Identify Licence Plates
Identify Clothing
Detect General Activity
Track Moving Targets
Track Through a Site



~



Limitations

LAW AND ORDER

South Australia's unluckiest rule breakers in 2019

These are the most unlucky South Australians in 2019. The rule breakers who were in the wrong place at the wrong time — including the one person caught buying alcohol for minors.

Unlucky rule breakers Pt 1.

Smoking within 10 metres of children's playground – **$270**

Be on bike path or footpath designed for bikes – **$111**

Having a passenger under 8 years old on a motorbike – **$200**

Having a (non-working) animal on public transport – **warning**

Holding a fireworks display without licence (under 3kg) – **warning**

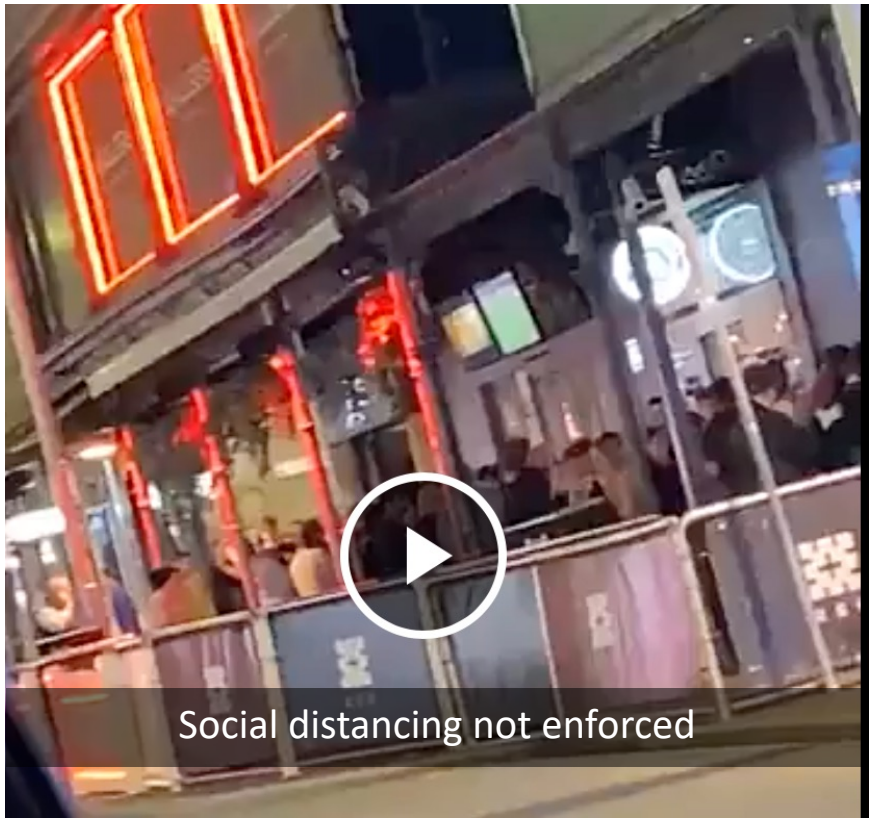
Contravene intervention order by failing to undergo assessment – **$220**

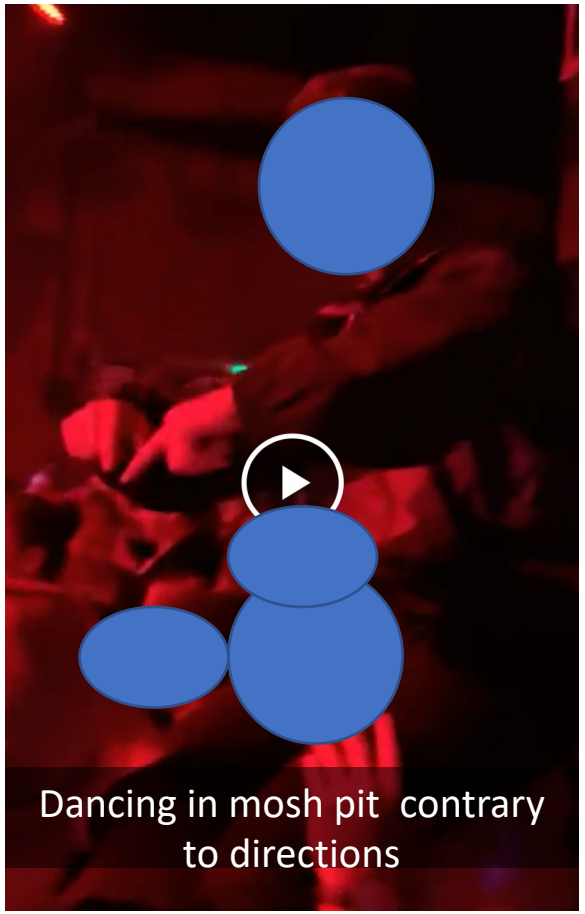
Coronavirus

Licensing boss warns venues after Red Square, Fat Controller avoid virus prosecution

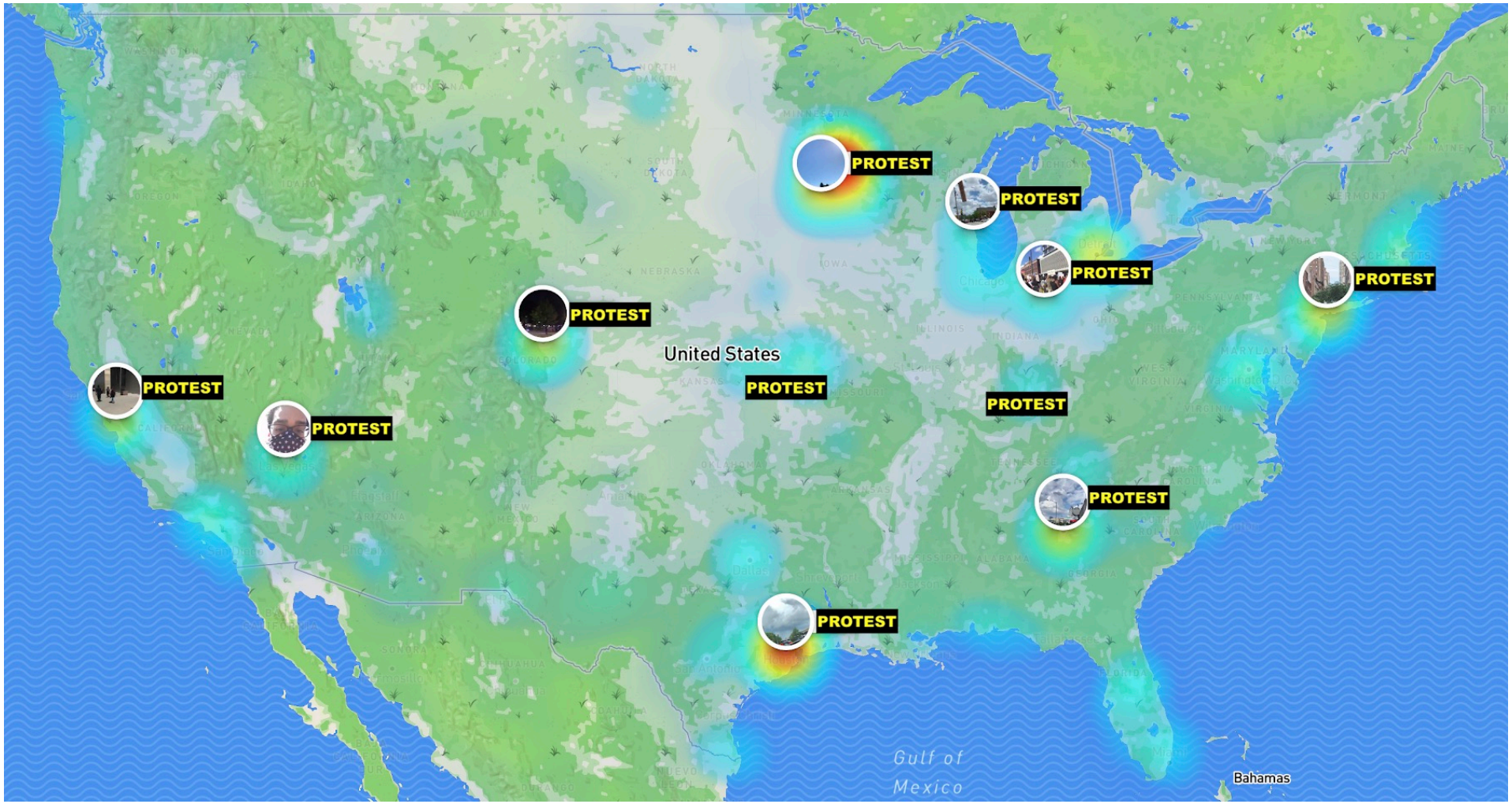
Detectives obtained Red Square footage showing the venue operating as a nightclub with drinking and dancing to loud amplified music. Footage showed revellers at Fat Controller dancing in a mosh pit.

Police fined both clubs $5060. After threatening to suspend their licences, Mr Soulio has now permitted them to trade under new operational plans.





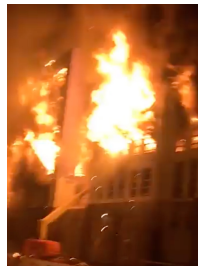
Limitations



Minneapolis-St Paul, May 2020








Extraction

	Extracted Media	Images	Videos
May 28	617	19	598
May 29	1434	39	1395
May 30	152	4	148
May 31	489	30	459
Total	2692	92	2600

I live in Minneapolis, Minnesota. Our community has been in the news recently because of the murder of George Floyd, the subsequent civil unrest, and the long-standing systemic racism within our community that has led to some of the greatest economic and educational disparities within the United States.

With the protests, riots, and looting following the murder of George Floyd, the situation in the Twin Cities (as our metro area is often called) was very unclear. I came across the work of Dr. Matthews when looking online for information about the riots and looting at 2 am.

Dr. Matthews used his Twitter feed to consolidate information from various technology sources, including Snapchat maps, public traffic cameras, and other technology, to provide up-to-the-minute information on what was happening. In the middle of the night when the rioting and looting were increasing, the local traditional media sources were silent. Dr. Matthews was using the technology resources available to communicate information on fires, protestors, and other activity. The local media was hours behind his posts, or missed information altogether. Having this near-live stream at a time when no other media was providing information critical to help us assess our safety risk and the impact on our community in the middle of our night.

…

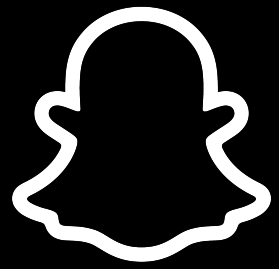
While we packed a bag in case we needed to flee, the information posted by Dr. Matthews allowed us to monitor the situation and determine if we needed to leave.

…

Dr. Matthews's tweets and the associated resources keep me connected to those who are leaving their homes to protest. I support the need for change, and know there are many others who demand change, not just in our local community, but around the world. Thank you.

WE WOULD LIKE TO MAKE THE FOLLOWING ACKNOWLEDGEMENTS

BUG BOUNTY FROM



hackerone

PRINCIPAL RESOURCES

THE UNIVERSITY of ADELAIDE