Reverse Engineering for the masses

Or how to empower gig economy workers and labour unions

Claudio Agosti and Gaetano Priori
staff@reversing.works

Reversing Works
37 Chaos Computer Congress

December 30, 2023

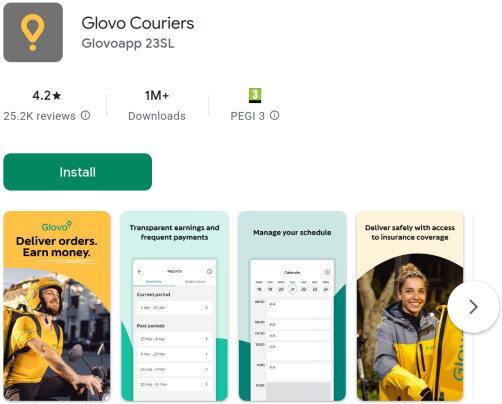
Agenda

1. Introduction
2. How it began
3. The Setup
4. The Results
5. Next Steps

1. Introduction

Problem Focus

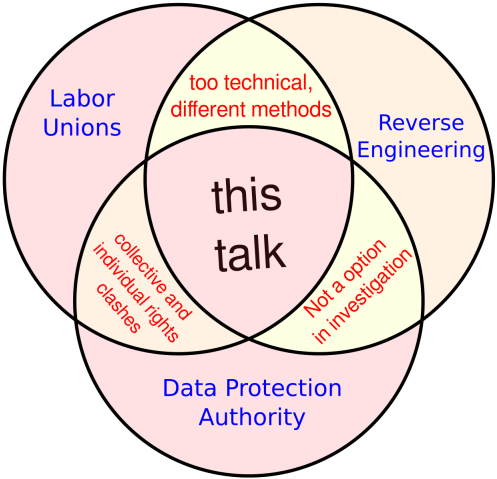
- We can use the terms 'gig economy' and 'platform workers' interchangeably.
- We acknowledge the significant impact this phenomenon has had, offering new jobs and creating new markets.
- In this talk, we argue that some practices embedded in these applications are problematic by design.



Who are we, and what can we do?

- Going back in time, we aim to reveal the hidden forms of power that platforms exert over workers.
- We believe that the algorithms, biases, and policies contain complex technocratic power dynamics, for which workers and their representatives, like unions, are often unprepared.
- We began with tracking.exposed in 2019, and since 2023 as **reversing.works**

A MULTIDISCIPLINARY EFFORT



2. How it began

A DSAR THAT NEVER WAS

- A rider got his account **deleted** from the Glovo app the day after he took part in a **strike**.
- The company blamed an unspecified "technical error" on the server side.
- In order to understand why he had been suddenly fired, his lawyer made a Data Subject Access Request to the company.
- The company answered that they only retained registration and contractual data basically.

We wanted to know more.

Or at least try to!

Looking at the app inner workings we can understand what data it collects and it retains

We found a volunteer who had a valid account that agreed to share it with us in order to make a complete assessment.

Additional challenges

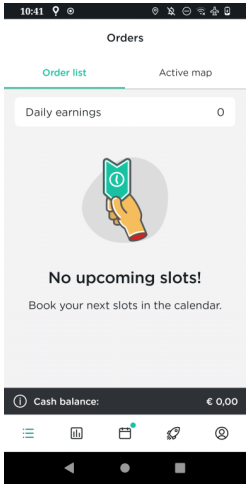
- We can not analyze the flow of data of a banned user.
- Also reproducing the same conditions for our volunteer is impossible.
- We decided so to make a privacy analysis in the context of the GDPR.

Fortunately there is an awesome ecosystem to analyze mobile apps!

3. The Setup

The setup

- I will run the Glovo mobile app on a clean Android device that I can control, recording everything the app does there.
- To gather enough data, we would have let the app for 48 hours without user interaction.
- To do this I used a build of Lineage OS 19 for raspberry pi, which allows to connect effortlessy remotely (by **adb** and **vnc**).



Permissions

What the app can see

Most sensitive device interactions are intermediated by the OS through permissions. Here we can see a sample from the **AndroidManifest**:

```
1    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
2    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
3    <uses-permission android:name="android.permission.CAMERA"/>
4    <uses-permission android:name="android.permission.ACCESS_GPS"/>
5    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
6    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
7    <uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION"/>
```

But how can we know which data is taken, when, and to whom it is sent?

A PRELIMINARY ANALYSIS OF THE APPLICATION CODE

- We began by statically analyzing the code of the application.
- In general this is useful to understand which compoments which components are implements, what is done using SDKs etc.
- We won't get all the information from here.

Runtime analysis

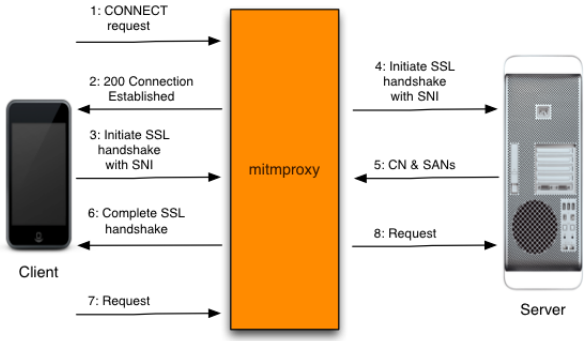
- To log every access to the device location we used Frida, an instrumentation framework with an excellent support for mobile applications.
- We won't dwelve here too much on how frida works, look at the Frida docs and if you want to go further read the awesome Frida Handbook.
- For example here we can see the script used to log every access to the Location service

```
Location.getLatitude.implementation = function(){
  console.log( "com.glovoapp.courier fetched Latitude : at: " + getLoggingDateAsString()+"\n");
}

Location.getLongitude.implementation = function(){
  console.log("com.glovoapp.courier fetched longitude : at: " + getLoggingDateAsString()+"\n");
}
```

Network Analysis

- Wireshark passive analysis
- Mitmproxy for TLS traffic inspection



From the Mitmproxy Docs

4. The Results

Firt results gained

Part 1: Location access history

July 2021

Thanks to location access logging we have been able to prove that the rider location was constantly taken, even outside working hours.

```
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched Latitude : 44.4969 at: Wed Jul 28 2021 01:58:44 GMT+0200
com.glovoapp.courier fetched longitude : 11.3515 at: Wed Jul 28 2021 01:58:44 GMT+0200
```

First results gained

July 2021

Part 2: Data sent to glovo, with an unknown score parameter.

```
2021-07-27 23:59:15 PUT https://api.glovoapp.com/v3/users/glv:courier
```

```
{
   "NIF": "REDACTED",
   "autoAssignentEnabled": true,
   "cityCode": "BOL",
   "description": null,
   "deviceUrn": null,
   "email": "REDACTED@gmail.com ",
   [...]
   "name": "REDACTED",
   "phoneNumber": {
       "countryCode": "IT",
       "number": "+39REDACTED"
   },
   [...]
   "rating": 4.5,
   [...]
}
```

Firt results gained

July 2021

Part 3: Data sent to third parties

POST https://sdk.fra-01.braze.eu/api/v3/data

```
    {
  [...]
  "app_version": "2.95.0",
  "app_version_code": "107830.0.0.0",
  "device_id": "f959377c-REDACTED",
  "events": [{
    "data": {
      "altitude": 282.6000061035156,
      "latitude": 44.4969,
      "ll_accuracy": 13.432000160217285,
      "longitude": 11.3515
    },
    "name": "lr",
    [...]
  }],

```

Repeating the tests a year after

September 2022

- We noticed that the proxy was not able to connect to *mParticle*, a third party tracker.
- We knew that the Glovo App used its SDK
- Looking further in the Wireshark network logs we noticed that the App was responding with a RST to the TLS handshake from our proxy.

Making more sense of it

September 2022

- The *mParticle* SDK was checking the signature of the TLS Certificate provided by the TLS Proxy.
- This technique is known as *certificate pinning*, and here is implemented using the **TrustManager**.

```
1 for (Certificate certificate : domain != null ?
      domain.getCertificates() : C4763d.m16361b())
       {
2     keyStore.setCertificateEntry(certificate.
      getAlias(), m16366a(certificateFactory,
      certificate.getCertificate()));
3 }
4 TrustManagerFactory trustManagerFactory =
      TrustManagerFactory.getInstance(
      TrustManagerFactory.getDefaultAlgorithm());
5 trustManagerFactory.init(keyStore);
6 SSLContext sSLContext = SSLContext.getInstance("
      TLS");
7 sSLContext.init(null, trustManagerFactory.
      getTrustManagers(), null);
8 this.f15711c = sSLContext.getSocketFactory();
```

The solution

And why Frida comes again in hand!

If you have seen the presentation *"Leveraging the use of dynamic instrumentation for pentesting mobile apps"* at this year's camp you already know that one of main usages of Frida is to bypass this kind of stuff!

```
try {
  var array_list = Java.use("java.util.ArrayList");
  var TrustManagerImpl_Activity = Java.use('com.android.org.conscrypt.TrustManagerImpl');
  TrustManagerImpl_Activity.checkTrustedRecursive.implementation = function(certs, ocspData, tlsSctData, host, clientAuth, untrustedChain, trustAnchorChain, used) {
    return array_list.$new();
  };
} catch (err) {
```

The final results

September 2022

POST nativesdks.mparticle.com/v2/36b7c1298092e74db9a90a2b03f6adf

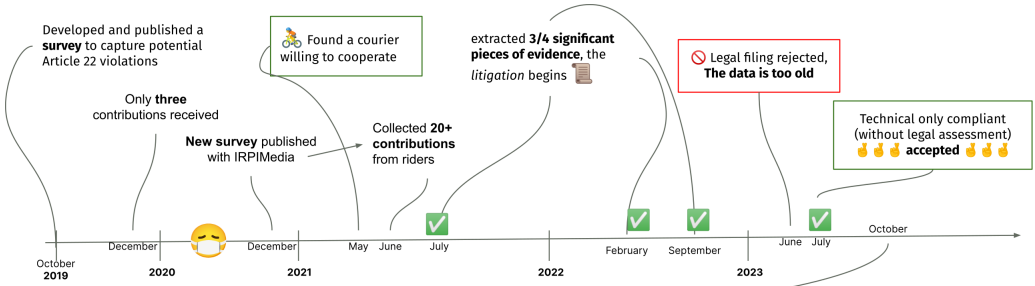
```
{
 [...]
      "dt": "e",
      "et": "Other",
      "n": "Gps state changed on the device",
      "attrs": {
      "lc": {
        "lat": 44.49711678040484,
        "lng": 11.352085079430195,
        "acc": 0
        "city": "BOL",
[...]
}
```

How the story goes

September 2022

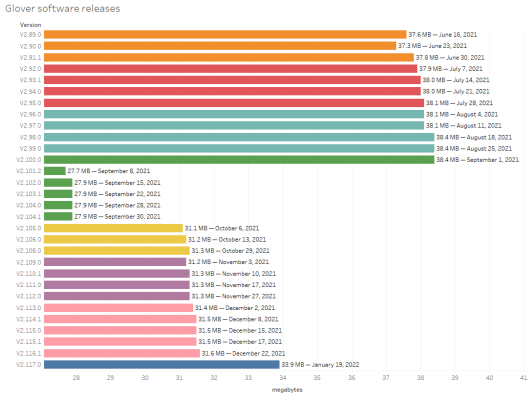
- By using reverse engineering techniques we have been able to prove that the company was constantly monitoring the position of the riders, even outside working hours, and was sharing their personal data, location included, with third parties.
- This evidence would have hardly come out of a DSAR to the company.
- We replicated the same analysis in July 2021, September 2022 and July 2023 finding similar results, to have a better perspective please read the paper that we have published with ETUI (Exercising workers' rights in algorithmic management systems)
- These results have resulted in a report to the Italian Data Protection Authority.

A 5 YEAR PERSPECTIVE



The side-challenge

- Data too old can't be considered also because the app changes (circa) **every week**
- .. at least, this suggest the potential violations weren't mistakes



A MEANINGFUL CONTEXTUAL INFORMATION

- In 2019 The Data Protection Authority launches investigations into numerous gig economy platforms operating in Italy.
- In 2021 Fines Glovo-Foodinho of 2.6 million€ (fine + prescritive measures)
- In 2022, Glovo wins the appeal and does not pay the fine
- In 2023 the Italian Supreme Court rejected the appeal and Glovo should pay the fine.

AI

Italy's DPA fines Glovo-owned Foodinho $3M, orders changes to algorithmic management of riders

Natasha Lomas @riptari / 1:30 PM GMT+1 • July 6, 2021

Comment

5. Next Steps

Lower the entrance barrier

- **exodus-privacy.org** is a great starting point; https://reports.exodus-privacy.eu.org/en/reports/search/com.glovoapp.courier/
- Privacy International released the **Data Interception Environment** https://privacyinternational.org/learn/data-interception-environment
- We at **reversing.works** wants to be technical providers of more specialized organizations that do field work (Unions?)
- At https://privacycamp.eu we organized a panel discussion (24 January, Streamed)

We're not alone, and we need to be more!

Workers Info Exchange
www.workerinfoexchange.org

Organize mutual aid, resources, and advocacy to improve conditions for all people using Amazon's Mechanical Turk
turkopticon.net

The Workers' Algorithm Observatory
wao.cs.princeton.edu

Digital permanence to retrieve your data, for the workers of the platforms Uber, Uber Eats, Smood.
personaldata.io/uber

Claudio Agosti and Gaetano Priori

Hamburg, December 30, 2023

staff@reversing.works