WORKER INFO EXCHANGE

December 2021 Report

Managed by Bots

Data-Driven Exploitation in the Gig Economy

Contents

Summary 3

Introduction 6

Part I: Misclassification 2.0: Controlled by Algorithm 10

Surveillance Arms Race 15

Surveillance Case Study I: Facial Recognition 17

Surveillance Case Study II: Geolocation Checks 22

Opaque Performance Management 25

Case Study: Algorithmic Control 27

Expansion of Law Enforcement Infrastructure 31

Case Study: Intelligence Sharing with Law Enforcement 33

Part II: Exercising Data Rights at Work: Access 41

Case studies: Individual DSARs 45

Circular and Futile Answers 46

Inconsistent and Incremental Data Sharing 49

Obfuscation and Resistance 50

Case studies: Platform Responses to Batch Requests by WIE 54

Deliveroo 56

Amazon Flex 56

Just Eat 57

Ola 57

Free Now 58

Bolt 60

Uber 63

Part III: Exercising Data Rights at Work: Strategic Litigation 68

Uber Drivers v. Uber I 71

Ola Drivers v. Ola 73

Uber Drivers v. Uber II 74

Appeals 75

London Licensing Appeal Cases 77

Conclusion 81

Summary

Employment in the so-called gig economy has boomed in recent years with the TUC reporting that 4.4 million people in the UK now work in the sector at least once per week. Large digital platforms have disrupted traditional players particularly in the taxi, private hire and logistics sectors with a business model of digitally mediated work and flexible labour terms.

The sector has been an employment rights battle ground as platforms sought to misclassify workers as independent contractors to avoid employer obligations, as well as tax and national insurance contributions. Having a huge workforce engaged on completely flexible terms has allowed platforms to rapidly scale and build competitive advantage from an excess supply of unpaid and underpaid workers who wait for work, while depressing their own wages.

A 2018 New School study of New York City drivers found that only 58% of a driver's time at work is utilised serving passengers. The rest of the time is spent waiting, unpaid, yet providing valuable immediacy to the platform. As the Employment Tribunal ruling in Aslam v Uber put it: "Being available is an essential part of the service drivers render to Uber." The ruling went on to quote Milton to illustrate the point: "They also serve who only stand and wait."

In the UK, Uber has chosen to cherry pick the recent Supreme Court ruling to refuse paying for waiting time. At the same time, our report shows that drivers are surveilled and subjected to algorithmic control even during this waiting time. Profiling used for automated work allocation determines how long or short the waiting will be for individual drivers. And where there is management control, there is an employment relationship which attracts rights for workers.

As case law has developed and platforms matured, employers have become more adept at hiding management control in automated algorithmic processes. The employment misclassification problem continues, but the mask rarely slips. To sustain the rights already hard won and to further secure the right of employment status, in one form or another, workers need to evidence management control.

The current situation for precarious workers in the gig economy is a dual challenge. Employment law and institutions of enforcement have been slow to tackle abuses of platform employers. Data protection law offers tools to protect the rights of individuals, however, there has not yet been adequate legal protection for digital rights at work, for individuals or the collective as represented by their trade unions.

For these reasons Worker Info Exchange was set up in 2019 as a digital rights NGO dedicated to research and advocacy of digital rights for workers and their trade unions. This report is an accounting of our experience so far in helping workers exercise their digital rights in the UK and the Netherlands, as well as other territories that have a European based data controller, including Australia.

Our aim is to develop a data trust to help disparate and distributed workforces to come together to aggregate their personal data at work and with a common understanding, begin the process of building real collective bargaining power. We believe worker data trusts and greater algorithmic transparency can go a long way to correcting the balance so workers can have a fairer deal.

However, just as gig economy platforms have resisted their responsibilities under employment law, our experience shows their compliance with data protection law has been poor. We have processed more than 500 subject access requests over the last eight months on behalf of workers at Amazon Flex, Bolt, Deliveroo, Free Now, Just Eat, Ola and Uber.

The persistent and widespread lack of compliance with data protection laws has hindered worker access to data and yielded almost no meaningful algorithmic transparency over critical worker management functions such as recruitment, performance management, work allocation and dismissals. The obfuscation and general lack of compliance has prevented us from reaching scale with a worker data trust. Instead, we have had to turn to strategic litigation across international boundaries to help workers once again secure their workplace rights.

On the other hand, driven by increasing pressure by transport regulators such as Transport for London and maturation of technology, we have seen widespread proliferation and a disproportionate use of worker surveillance in the name of fraud prevention. In our opinion, the management of 'fraud' is often conflated with performance management rather than detection of actual criminal fraud. An example of this is where worker fraud probability scores are inappropriately used in automated work allocation decisions by a number of apps.

In the UK, these already weak digital rights for workers will be fatally compromised if the government's proposals on GDPR divergence are passed into law. The proposals would give employers more discretion in how or whether to respond to data access requests and to charge a fee for doing so. There is also a proposal to strip out the current Article 22 protections that allow workers to know how they have been subjected to automated decision making and the likely effect of such, the right to challenge such decisions and the right to give your point of view.

The government also plans to reduce the obligation on employers to prepare data protection impact assessments (DPIA) before the processing of highly sensitive personal data, which is routinely carried out by gig employers for facial recognition identity checks, location tracking and anti-fraud surveillance. This would be a hammer-blow for precarious workers who already have long been denied basic employment rights who could now be robbed of the means to hold rogue employers to proper account.

Given the threats to and shortcomings in GDPR implementation, many jurisdictions, such as the EU as well as some US states, are currently considering greater employment rights protections for gig workers that address the issues arising from algorithmic management. In the UK, the TUC have published an AI Manifesto, proposing a series of amendments to employment and data protection law to promote greater transparency and equality in digitally mediated work. We strongly support the call for greater digital rights protections.

This report was written by Cansu Safak and James Farrar

With thanks to Anton Ekker for his contributions, and the App Drivers and Couriers Union (ADCU), Bama Athreya and Yaseen Aslam for their ongoing support.

This work was made possible by support from the Mozilla Foundation, Digital Freedom Fund and Open Society Foundations

Illustrations by Célune Gabriella Ama Acheampong and Avantika Mohapatra
Graphic Design by Célune Gabriella Ama Acheampong

Introduction

The past year has marked a turning point for gig platform workers in the realisation of their employment and digital rights. The practice of digitally mediated work has led to a convergence of employment and data protection rights and the increasing litigation and advocacy activity by workers has been yielding results in these domains. Across Europe, courts have passed several significant judgments recognising the exploitative role of algorithmic management practices by gig platforms while also condemning the lack of fairness and transparency in such automated systems.

In Italy, the Bologna court ruled that Deliveroo's rating system had discriminated against workers while the data protection authority, Garante, served two GDPR fines to Deliveroo and Glovo due to their failure to adequately disclose the workings of their job allocation and performance management algorithms. Spain passed the first legislation to attempt to regulate AI in the area of employment, establishing both worker status for gig workers and the right to be informed about the rules and parameters of the algorithms they are subject to - unleashing a torrent of complaints. This resulted from yet another court case against Glovo that ended up in the Spanish Supreme Court.

Along with these high-profile decisions, the UK Supreme Court also concluded this year that Uber drivers were party to a transportation service that is "very tightly defined and controlled by Uber" betraying a clear employment relationship, which the company claimed did not exist in its endeavour to (mis)classify the workers as independent contractors. Significantly, evidence of this relationship comes from the data driven systems rideshare platforms use to manage their workforces.

Some of the issues highlighted by the UK Supreme Court related to the management of drivers through the algorithmic monitoring of job acceptance rates, route choices, driving behaviour and customer ratings. However, even though there is greater recognition of algorithmic management, the recent gains in the courts do not fully protect workers against its harms. The limb (b) worker status given to Uber drivers as a result of the Supreme Court decision is an intermediary status between contractor and employee, and still falls short of shielding them from unfair dismissals, for example.

Our experience suggests that these algorithmic management tools, with the addition of intensifying surveillance practices, continuously scrutinising workers for potential fraud or wrongdoing, are resulting in a deeply exploitative working environment. We are seeing an inordinate number of automated dismissals across the entire gig industry, many of which we believe to be unlawful according to Article 22 of the General Data Protection Regulation (GDPR).

Article 22 does provide workers with some limited protections against the adverse effects of automated decision making and profiling, through the right to obtain human intervention and contest the decision. Article 15 of the GDPR guarantees the right to be informed about the existence of such automated decision making and to be provided with meaningful information about the logic of processing.

Taking these rights as a basis, Worker Info Exchange was set up with the mission of supporting gig workers in navigating this complex and under regulated space. The goal and remit of our work is to test whether these GDPR instruments can be utilised to address unfair employment practices and expand the scope of the data made available to individuals in their capacity as workers. In other words, our ambition is to use data access as a method of building collective worker power for testing mechanisms of redress in a digitally mediated labour market.

When the employment relationship between the gig platform and the worker is executed through extensive data collection and analysis, employment rights become inextricably linked with the exercise of data rights. Gig platforms assert control over workers by maintaining an informational asymmetry, and data access can provide a means of exposing the power (im)balance generated by the informational gap between gig platforms and their workers. Getting access to personal data can allow workers to make independent evaluations about their working conditions and answer questions concerning their pay calculations, the quality and quantity of work offered, as well as challenging the grounds for adverse performance management including suspension and dismissal.

Our goal in facilitating data access is to create collective stores of data to develop a greater understanding of working conditions and consequently bargaining power. In recent years, a number of noteworthy initiatives have emerged operating with similar aims but using different methodologies for retrieving data. Some projects in this field run their own data collection and analytics on earnings and performance to assess the fairness of labour conditions (for example Driver's Seat Coop and WeClock, among others.)

These all present unique insights into the gig economy and should be thought of as constituting a continuum of data practice. We have approached this issue by demanding that platforms share the data that workers are legally entitled to, however this has introduced additional obstacles to the larger goal of collectivising data. We took this route because we wished to set standards and precedents in data protection law, but also because we believe there are certain types of information that can only be obtained by requesting the data directly from the platforms.

We have found, particularly in the case of surveillance fuelled allegations of irregular activity and fraud, that it is necessary to have the data held by the companies to understand and contest the accusations. Data access can help us unearth the inconsistencies in the narratives advanced by platform companies and help shift the burden of proof from the workers back on to the platforms.

From this perspective, the endeavour of demanding platform data has proven extremely successful in resolving numerous employment disputes. The simple demonstration of platforms' refusal to provide personal data has reversed several license revocations (enforced by TfL) in court and thus become an additional tool in the exercise of employment rights.

This constitutes the other branch of activity for Worker Info Exchange; as we are frustrated in our attempts to gain clarity and transparency over the complex systems determining workplace conditions, we frequently need to resort to litigation and turn to courts for decisions in the emergent field of digital labour rights. The artificial 'data crisis' the gig platforms have created is in many ways an attempt to exhaust and deplete the resources of precarious workers and unions alike by drawing disputes into courts where they can be prolonged and the accountability for corporate misconduct delayed.

In line with these strands of activity, this report is written in three parts: The first section explores different facets of algorithmic management and its harms, with associated case studies. The second section deals with our process in utilising Data Subject Access Requests (DSARs) while the third offers an overview of the GDPR related cases we have taken forward in Amsterdam, as well as the licensing cases we are supporting in London. We hope this report will demonstrate the current state of play in the exercise of rights at the intersection of data and labour and reveal the cumulative effects of repeated non-compliance by gig platforms.

"Platform companies are operating in a lawless space where they believe they can make the rules. Unfortunately this isn't a game; virtual realities have harsh consequences for gig workers in real life. What's encouraging is that workers themselves are not waiting for laws, policymakers or even allies in the human rights movement to rescue them. Gig workers are organizing and using their collective voice to demand new protections that are fit for purpose in a digitizing economy."

Bama Athreya, Fellow, Open Society Foundations

Part I

Misclassification 2.0
Controlled by Algorithms

Overview

In the six year battle for worker rights in the UK's gig economy, Uber argued that it was merely the agent of the self employed driver doing nothing more than passively booking work orders and collecting payment. To advance this fiction, gig platforms set up elaborate contracts that make it appear as though the driver and passenger are transacting directly with each other, when in fact all passenger information is closely shielded by companies. Uber, for example, generates a notional invoice on behalf of the driver to every passenger they carry. The invoice will cite only the passenger's first name and is never actually sent to the customer.

These misclassification techniques, commonly used across the gig economy, enable platforms to avoid employer legal responsibilities such as basic worker rights protections and national insurance contributions. In the UK it has also enabled platform companies to avoid value added sales tax (VAT). But earlier this year, the Supreme Court affirmed the right of the lower courts to discard artificial contracts and to determine the true nature of the employment relationship based on the evidence of a management relationship of control over workers.

As platform companies conclude that using misleading contracts is no longer viable as a method of employment misclassification, they will be tempted to double down on process automation for the concealment of management control. Algorithmic control becomes misclassification 2.0. Indeed, there is ample evidence that this is already happening. Gig platforms are more determined than ever to pursue misclassification strategies so that they can continue to control the workforce while avoiding the risk that drivers might graduate from 'worker' status with limited rights to employee status with substantially more rights.

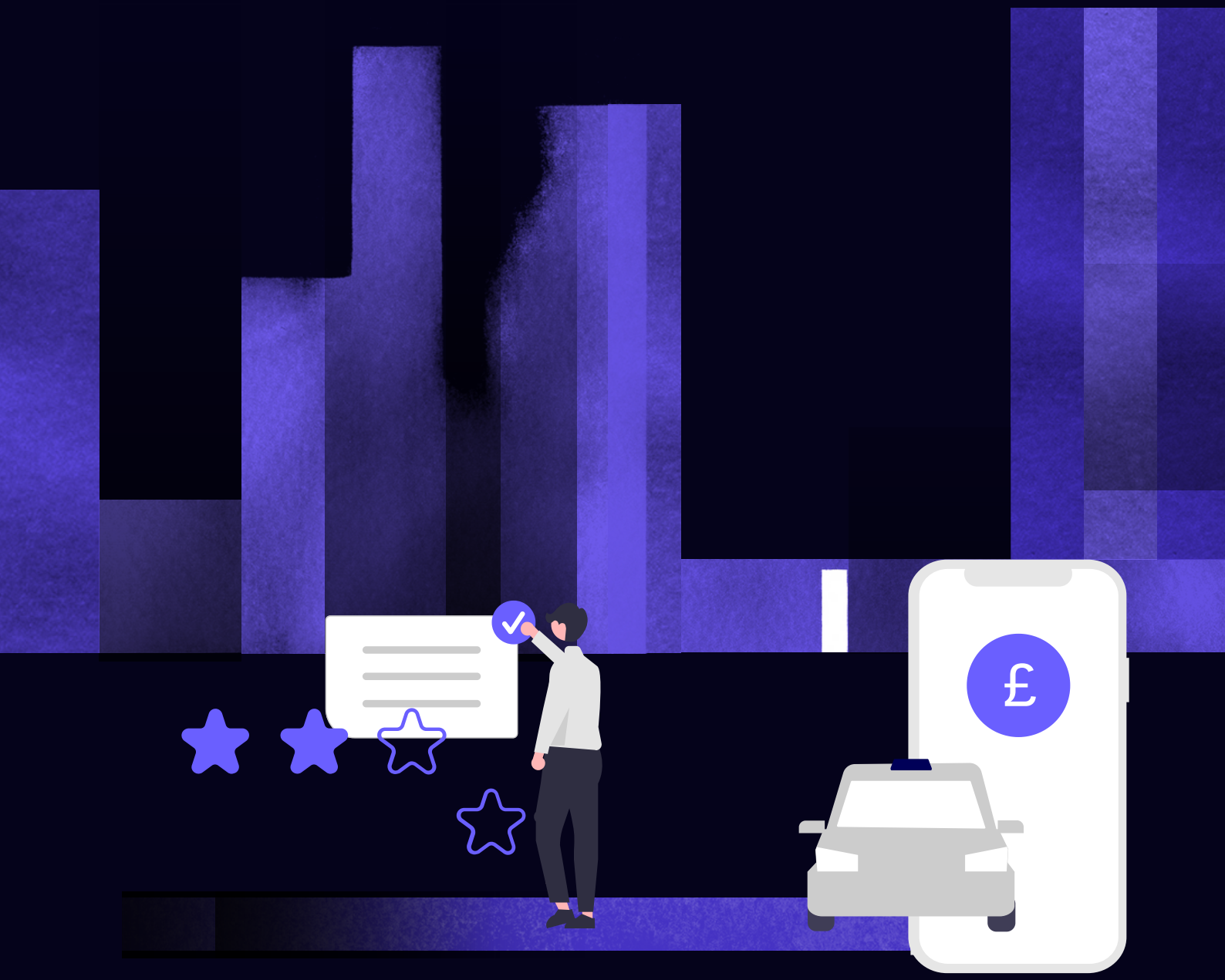
So what is algorithmic control and what are the specific risks for gig workers? In the ride-share and delivery industries specifically, the means of algorithmic management of greatest concern to us include the following:

Surveillance

Intrusive surveillance for the stated purpose of security and identification. This encompasses the use of fraud detection and facial recognition technologies. We are aware that surveillance is conducted even when the worker has not logged in to make themselves available for work. It also includes surveilling the worker's use of the app as a consumer.

Work allocation

Uber has until very recently insisted that work allocation is decided on the proximity of drivers and passengers to each other however now states that past behaviour and preferences are factored in. Ola uses driver profiles which include 'fraud probability scores' in automated decision making for work allocation.



Performance management

Assessment of work performance includes but is not limited to monitoring of driving behaviour including ETA, customer ratings, job acceptance & completion rates, interaction with support staff, availability.

Pricing

Closely related to work allocation is automated price setting. Perhaps the most well-known method is Uber's so called 'surge' or 'dynamic pricing' which purports to clear market demand with real time, local price fluctuations.

The management decisions above are mostly automated or semi-automated with limited human intervention. Business models of the gig economy rely on mass automation of management decisions and workplace supervision. While some employers are reticent on this point, Deliveroo has been quite forthright about it in their rider privacy policy:

"Given the volume of deliveries we deal with, we use automated systems to make the automated decisions described above as they provide a more accurate, fair and efficient way of identifying suspected fraud, preventing repeated breaches of your Supplier Agreement and limiting the negative impact on our service.

Human checks would simply not be possible in the timeframes and given the volumes of deliveries that we deal with."

Deliveroo's Privacy Policy

Surveillance Arms Race

We have been seeing a surveillance arms race in the gig economy since Uber introduced its so-called Hybrid Real Time Identification System during 2020. Just one day before Transport for London (TfL) announced its decision to refuse renewal of their license in November 2019, Uber offered to introduce this surveillance system which incorporates facial recognition with GPS monitoring.

This was in response to TfL's complaint that 21 drivers had been detected (out of 90,000 analysed over several years) as engaged in account sharing which allowed potentially unlicensed and uninsured drivers to illegally offer their services on the app. The activity was made possible by resetting the GPS location of the device as outside the UK, where it is possible for drivers to upload their own photos. This gap was quickly closed by Uber and the activity detected was vanishingly small compared to the scale of Uber's operation. The introduction of facial recognition technology by the industry has been entirely disproportionate relative to the risk perceived. Nevertheless, the requirement for real time identification went on to become a condition of Uber's license renewal at the Westminster Magistrates Court in September 2020.

In the case of Uber, both the platform's management and TfL have failed to ensure that appropriate safeguards were put in place to protect the rights and freedoms of drivers despite TfL having reviewed the data protection impact assessment for the technology in March 2020. According to TfL reports, 94% of private hire vehicle (PHV) drivers are from black and ethnic minority backgrounds and the introduction of this technology, which is well recognised for its low accuracy rates within these groups, has proven disastrous for vulnerable workers already in precarious employment.

Bolt has since announced that it was investing €150 million in AI driver anti-fraud detection systems including facial recognition. Deliveroo announced that they too would introduce facial recognition identity checks. Ola Cabs has also rolled out facial recognition identification as a feature of its Guardian system, incorporating machine learning which they claim enables them to "continuously learn and evolve from millions of data points every single day, to improve risk signalling and instant resolution."

Free Now, a Daimler and BMW joint venture, also closely surveils drivers as part of its fraud prevention programme. Indeed, in documents filed by Free Now with the High Court in a Judicial Review of TfL's decision to grant them a license in London, they disclosed that TfL has made monthly reports of driver dismissals for various reasons (including 'fraudulent activity') a condition of their recent license renewal. But the description of the data processed for the purpose of fraud prevention raises more questions than is answered by Free Now's privacy policy.

In this document, Free Now states that they use a 'random forest' algorithm to produce a fraud score which they use to "prioritise the dispatched journeys accordingly. This ensures a fair and risk minimised dispatchment." Free Now contested their use of this fraud detection system when we inquired about it in June 2021, claiming that this section of the privacy policy was outdated (please see company case study in part II of the report.) However, the reference to this system remained in the policy, despite an update made in September 2021. We shared our report with Free Now in November and highlighted this discrepancy. Free Now has now removed the description of the 'random forest' algorithm, but continues to use GPS location data for fraud prevention purposes.

What is particularly concerning about the use of these systems is that they conflate fraud management with performance management. The fact that such 'fraud' indicators are used as variables for work allocation and that the behaviours generating them are allowed to continue on the platform demonstrates that these are not instances of criminal fraud, but mechanisms of control, which assess how well workers are performing against the opaque metrics set by companies. We suggest that any 'fraud' terminology used in these contexts also function as part of the misclassification game, designed to conceal the employment relationship.

Surveillance Case Study I

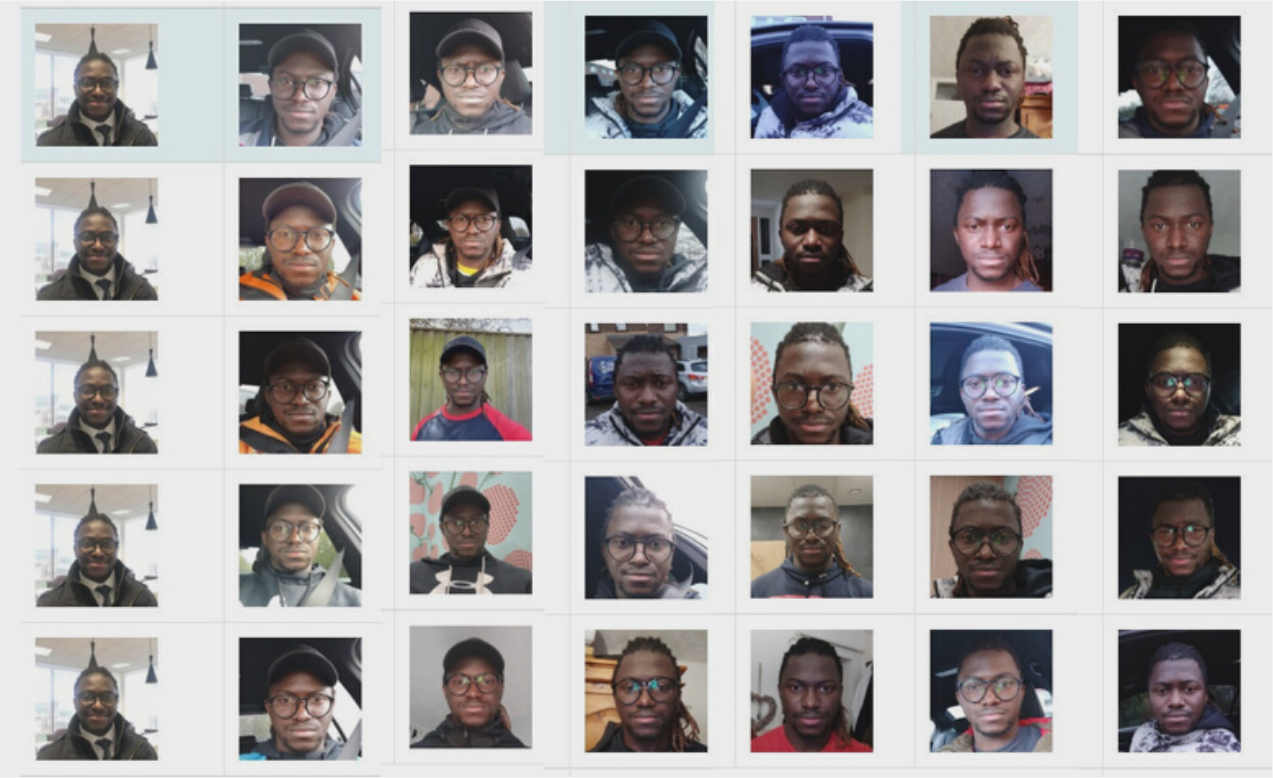
Facial Recognition

Watch interview

In April 2020, Uber introduced a Real Time ID (RTID) system in the UK which uses a combination of facial verification and location checking technologies to authenticate drivers' identities and prevent them from sharing access to their accounts. The RTID system incorporates Microsoft's FACE API, facial recognition software and requires drivers and couriers to periodically take real-time selfies to continue using the Uber app. The photo is then checked against the driver's account profile picture (and in some jurisdictions, against public databases to "prevent identity borrowing or to verify users' identities.")

Pa Edrissa Manjang had been working with Uber for about a year when he was deactivated due to a selfie verification failure. While Uber drivers and couriers routinely provide selfies, these are not stored on the workers' phones and they cannot retain the evidence of their submissions. Pa was not given any warnings or notified of any issues until his dismissal; the Real Time ID verification system appeared to approve all of his photographs with a green check.

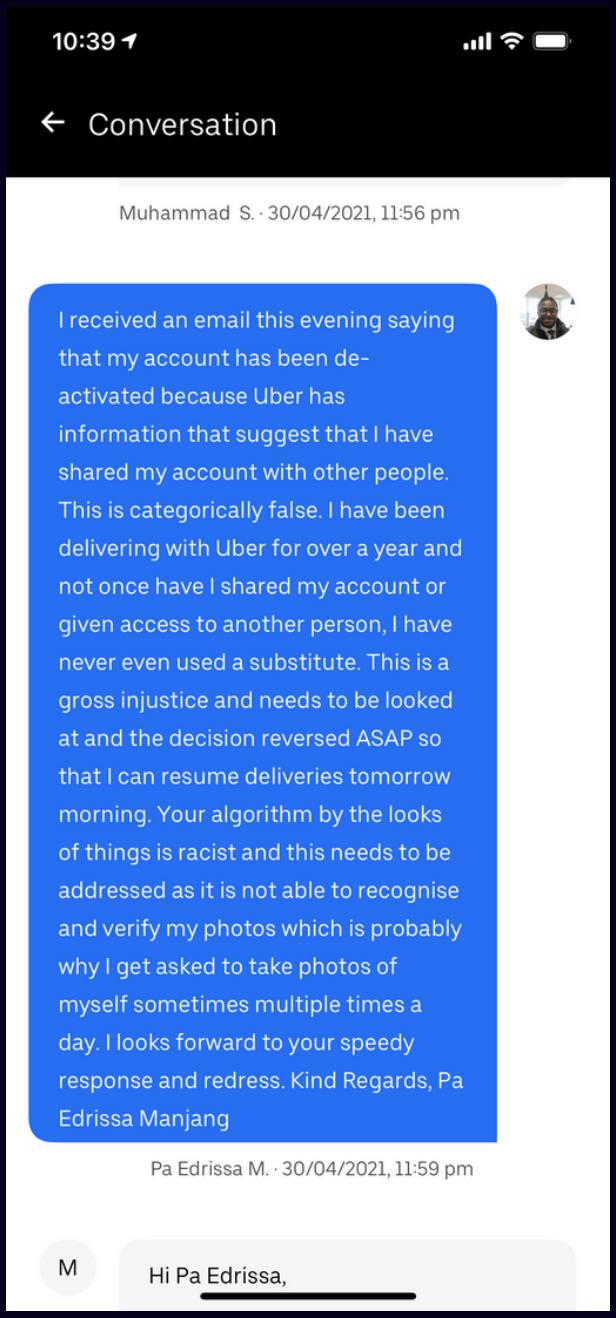
Following his dismissal, Pa sent numerous messages to Uber to rectify the problem, specifically asking for a human to review his submissions. Each time Pa was told "we were not able to confirm that the provided photos were actually of you and because of continued mismatches, we have made the final decision on ending our partnership with you." We obtained the selfies in question through a subject access request, which revealed that all of the photos Pa submitted were in fact of him. This was the first instance in which we succeeded in obtaining the selfies submitted by a courier or driver. It is unclear why this request succeeded when many before it failed.

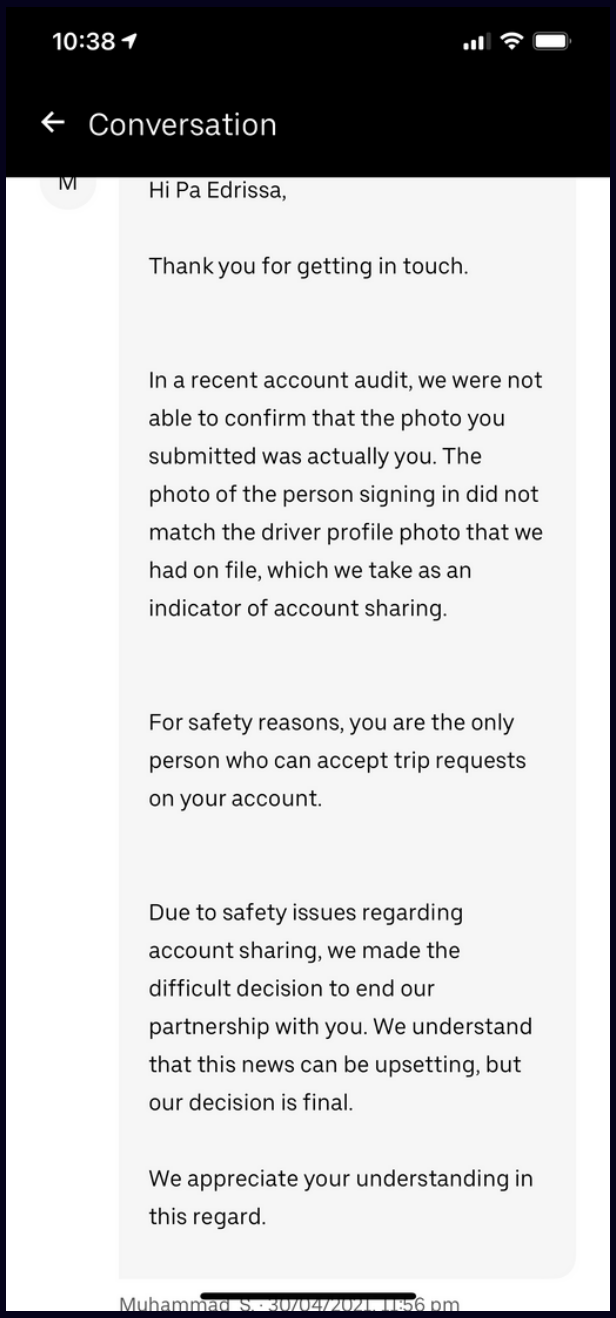


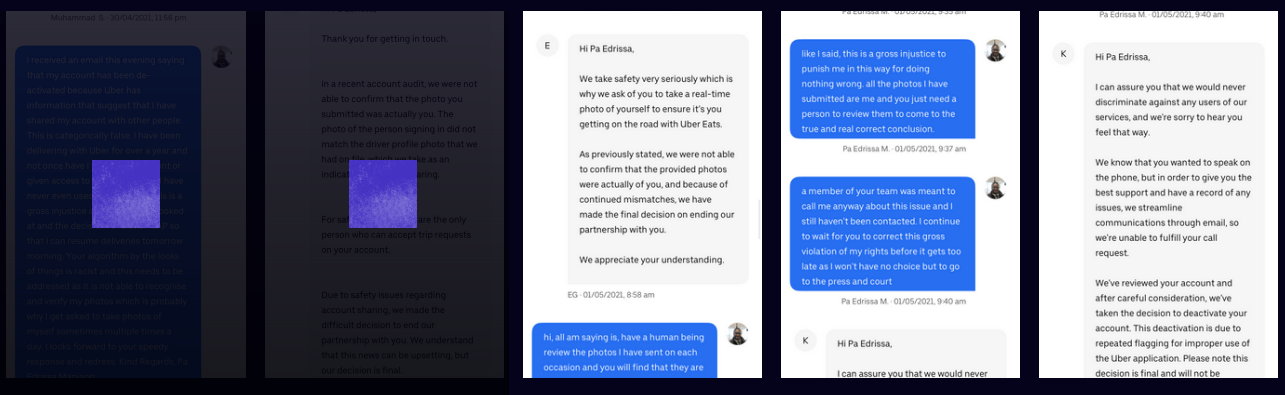
We also wrote to Microsoft earlier in the year to raise our concerns regarding Uber's unregulated use of FACE API across its platform. In response, Microsoft stressed that all parties involved in the deployment of such technologies have responsibilities which include: "incorporating meaningful human review to detect and resolve cases of misidentification or other failure" and "to provide support to people who believe their results were incorrect; and to identify and address fluctuations in accuracy due to variation in conditions." Pa's case suggests that these crucial checks have not been implemented in the processing of RTID images.

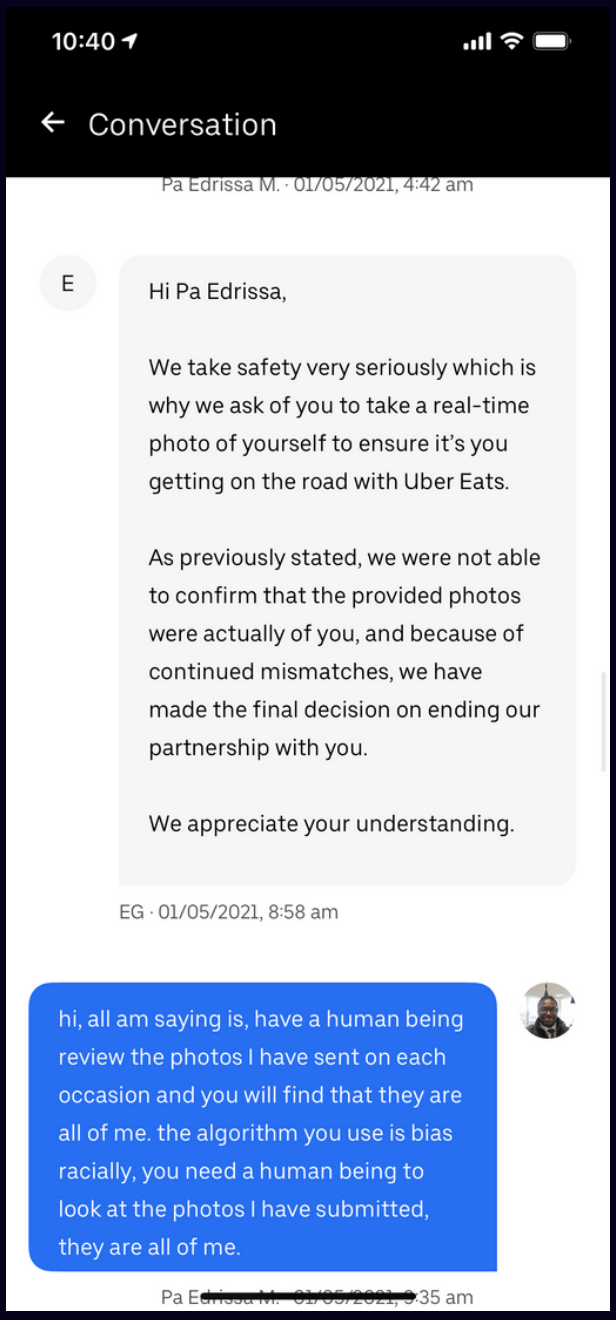
When asked about the human review process and the facial recognition issues outlined in this case study, Uber claimed that all human reviewers take a test developed by cognitive psychologists to qualify as reviewers and go through additional training in the form of weekly coaching and quality audits. Uber also stated that they had conducted internal fairness tests on their 'facial verification' technology and "found no evidence that the technology is flagging people with darker skin complexions more often, nor that it is creating longer waiting times due to additional human review."

Pa is now bringing a case against Uber to challenge its racially discriminatory facial recognition deployment, represented by Bates Wells, with support from the Equality and Human Rights Commission, the App Drivers and Couriers Union and Worker Info Exchange.

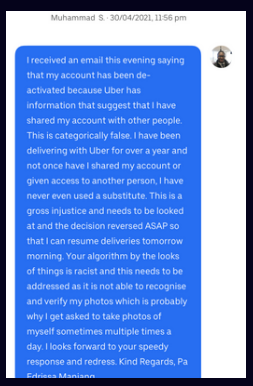

10:39
Conversation
Muhammad S. · 30/04/2021, 11:56 pm
I received an email this evening saying that my account has been de-activated because Uber has information that suggest that I have shared my account with other people. This is categorically false. I have been delivering with Uber for over a year and not once have I shared my account or given access to another person, I have never even used a substitute. This is a gross injustice and needs to be looked at and the decision reversed ASAP so that I can resume deliveries tomorrow morning. Your algorithm by the looks of things is racist and this needs to be addressed as it is not able to recognise and verify my photos which is probably why I get asked to take photos of myself sometimes multiple times a day. I looks forward to your speedy response and redress. Kind Regards, Pa Edrissa Manjang
Pa Edrissa M. · 30/04/2021, 11:59 pm
M
Hi Pa Edrissa,

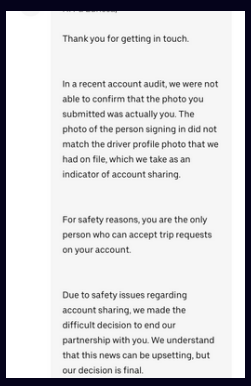

10:38
Conversation
M
Hi Pa Edrissa,
Thank you for getting in touch.
In a recent account audit, we were not able to confirm that the photo you submitted was actually you. The photo of the person signing in did not match the driver profile photo that we had on file, which we take as an indicator of account sharing.
For safety reasons, you are the only person who can accept trip requests on your account.
Due to safety issues regarding account sharing, we made the difficult decision to end our partnership with you. We understand that this news can be upsetting, but our decision is final.
We appreciate your understanding in this regard.

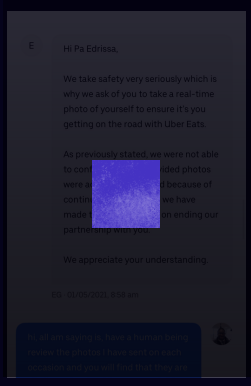


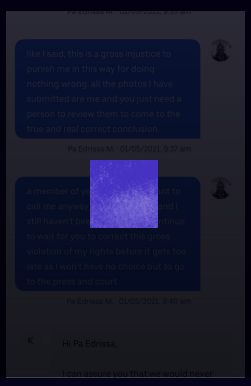

10:40
Conversation
Pa Edrissa M. · 01/05/2021, 4:42 am
E
Hi Pa Edrissa,
We take safety very seriously which is why we ask of you to take a real-time photo of yourself to ensure it's you getting on the road with Uber Eats.
As previously stated, we were not able to confirm that the provided photos were actually of you, and because of continued mismatches, we have made the final decision on ending our partnership with you.
We appreciate your understanding.
EG · 01/05/2021, 8:58 am
hi, all am saying is, have a human being review the photos I have sent on each occasion and you will find that they are all of me. the algorithm you use is bias racially, you need a human being to look at the photos I have submitted, they are all of me.
Pa Edrissa M. · 01/05/2021, 9:35 am

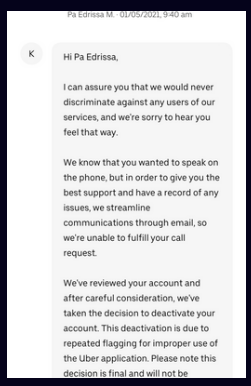

10:52
4G
Conversation
Pa Edrissa M. · 01/05/2021, 9:35 am
like I said, this is a gross injustice to punish me in this way for doing nothing wrong. all the photos I have submitted are me and you just need a person to review them to come to the true and real correct conclusion.
Pa Edrissa M. · 01/05/2021, 9:37 am
a member of your team was meant to call me anyway about this issue and I still haven't been contacted. I continue to wait for you to correct this gross violation of my rights before it gets too late as I won't have no choice but to go to the press and court
Pa Edrissa M. · 01/05/2021, 9:40 am
K
Hi Pa Edrissa,
I can assure you that we would never discriminate against any users of our services, and we're sorry to hear you feel that way.
We know that you wanted to speak on

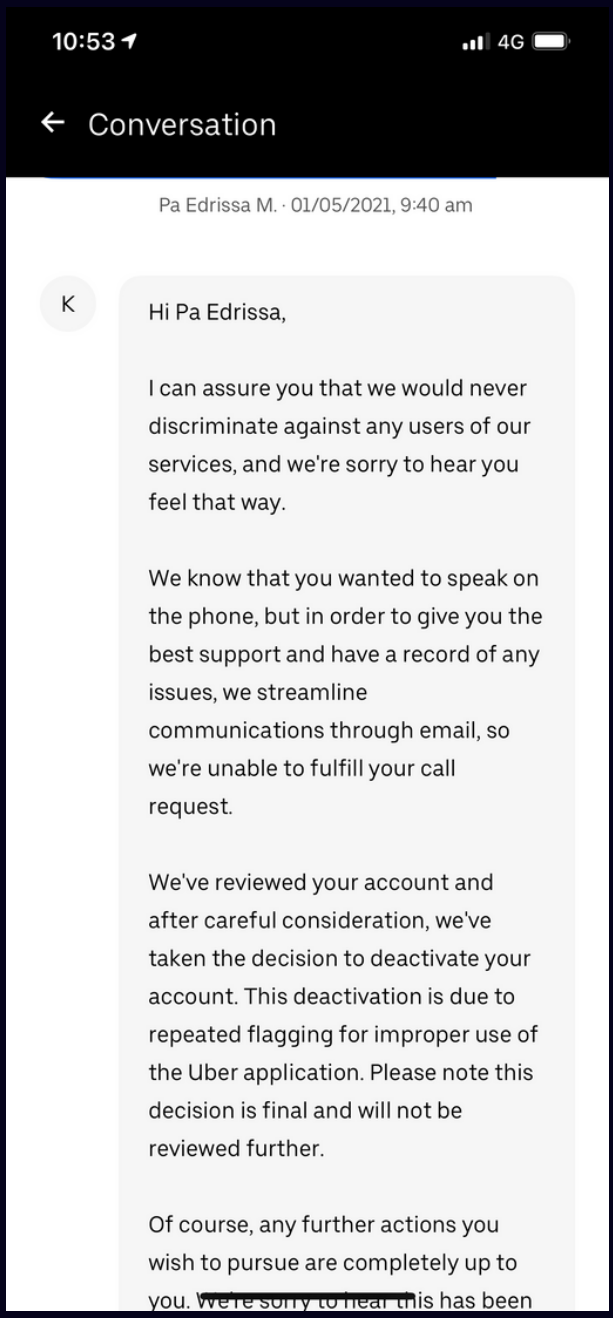

Muhammad S. · 30/04/2021, 11:56 pm
I received an email this evening saying that my account has been de-activated because Uber has information that suggest that I have shared my account with other people. This is categorically false. I have been delivering with Uber for over a year and not once have I shared my account or given access to another person, I have never even used a substitute. This is a gross injustice and needs to be looked at and the decision reversed ASAP so that I can resume deliveries tomorrow morning. Your algorithm by the looks of things is racist and this needs to be addressed as it is not able to recognise and verify my photos which is probably why I get asked to take photos of myself sometimes multiple times a day. I looks forward to your speedy response and redress. Kind Regards, Pa

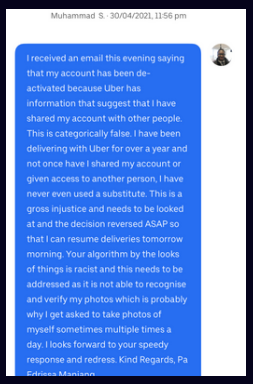

Thank you for getting in touch.
In a recent account audit, we were not able to confirm that the photo you submitted was actually you. The photo of the person signing in did not match the driver profile photo that we had on file, which we take as an indicator of account sharing.
For safety reasons, you are the only person who can accept trip requests on your account.
Due to safety issues regarding account sharing, we made the difficult decision to end our partnership with you. We understand that this news can be upsetting, but our decision is final.

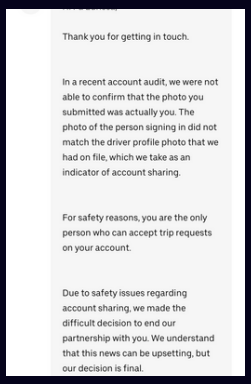


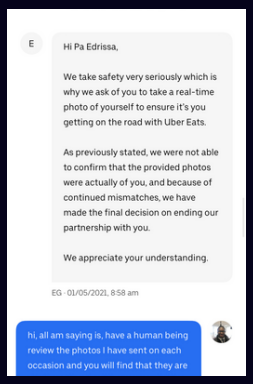


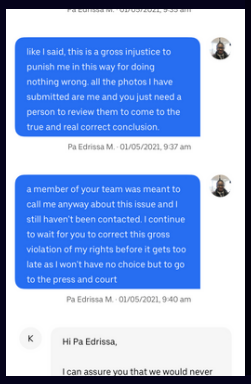

Pa Edrissa M. · 01/05/2021, 9:40 am
K
Hi Pa Edrissa,
I can assure you that we would never discriminate against any users of our services, and we're sorry to hear you feel that way.
We know that you wanted to speak on the phone, but in order to give you the best support and have a record of any issues, we streamline communications through email, so we're unable to fulfill your call request.
We've reviewed your account and after careful consideration, we've taken the decision to deactivate your account. This deactivation is due to repeated flagging for improper use of the Uber application. Please note this decision is final and will not be

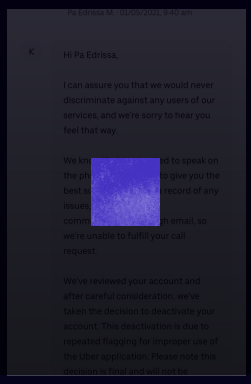

10:53
4G
Conversation
Pa Edrissa M. · 01/05/2021, 9:40 am
K
Hi Pa Edrissa,
I can assure you that we would never discriminate against any users of our services, and we're sorry to hear you feel that way.
We know that you wanted to speak on the phone, but in order to give you the best support and have a record of any issues, we streamline communications through email, so we're unable to fulfill your call request.
We've reviewed your account and after careful consideration, we've taken the decision to deactivate your account. This deactivation is due to repeated flagging for improper use of the Uber application. Please note this decision is final and will not be reviewed further.
Of course, any further actions you wish to pursue are completely up to you. We're sorry to hear this has been


Muhammad S. · 30/04/2021, 11:56 pm
I received an email this evening saying that my account has been de-activated because Uber has information that suggest that I have shared my account with other people. This is categorically false. I have been delivering with Uber for over a year and not once have I shared my account or given access to another person, I have never even used a substitute. This is a gross injustice and needs to be looked at and the decision reversed ASAP so that I can resume deliveries tomorrow morning. Your algorithm by the looks of things is racist and this needs to be addressed as it is not able to recognise and verify my photos which is probably why I get asked to take photos of myself sometimes multiple times a day. I looks forward to your speedy response and redress. Kind Regards, Pa


Thank you for getting in touch.
In a recent account audit, we were not able to confirm that the photo you submitted was actually you. The photo of the person signing in did not match the driver profile photo that we had on file, which we take as an indicator of account sharing.
For safety reasons, you are the only person who can accept trip requests on your account.
Due to safety issues regarding account sharing, we made the difficult decision to end our partnership with you. We understand that this news can be upsetting, but our decision is final.


E
Hi Pa Edrissa,
We take safety very seriously which is why we ask of you to take a real-time photo of yourself to ensure it's you getting on the road with Uber Eats.
As previously stated, we were not able to confirm that the provided photos were actually of you, and because of continued mismatches, we have made the final decision on ending our partnership with you.
We appreciate your understanding.
EG · 01/05/2021, 8:58 am
hi, all am saying is, have a human being review the photos I have sent on each occasion and you will find that they are


like I said, this is a gross injustice to punish me in this way for doing nothing wrong. all the photos I have submitted are me and you just need a person to review them to come to the true and real correct conclusion.
Pa Edrissa M. · 01/05/2021, 9:37 am
a member of your team was meant to call me anyway about this issue and I still haven't been contacted. I continue to wait for you to correct this gross violation of my rights before it gets too late as I won't have no choice but to go to the press and court
Pa Edrissa M. · 01/05/2021, 9:40 am
K
Hi Pa Edrissa,
I can assure you that we would never



Surveillance Case Study II

Geolocation Checks

While the use of flawed facial recognition systems is undoubtedly problematic, we have also seen many drivers dismissed following false accusations from Uber that they were engaged in fraudulent account sharing, due to two devices being detected by Uber in two locations at the same time. In all the cases we have analysed, we have found that the problem is related to the driver having installed the app on two devices for convenience but with only one of the devices logged-in for work.

Just before 8 pm on September 11, 2020 and Aweso Mowlana was working for Uber in South London. He was a 4.95 star rated driver who had conducted more than 11,500 trips in over 5 years working for Uber. Aweso had just dropped a passenger near Elephant and Castle when he logged-off for a short break. Like many drivers, Aweso had installed the app on a second device which was an iPhone. This particular evening he had left the iPhone at home and was working with his other phone, a Samsung.

At 8:02 pm Aweso attempted to log back into the Uber app to make himself available for his next job. Before he was allowed to log back in, he was prompted to provide a selfie as part of Uber's Real Time Identity Check (RTID). His photo matched Uber's reference photo so he successfully completed the log-in procedure to continue his shift. But unknown to him, Uber systems had either detected and/or pinged his second phone. Earlier that day, his son had picked up his second phone by mistake and taken it with him to his girlfriend's house in Uxbridge. Uber later said they requested an RTID check from this device at 8:03 pm but by this time Aweso was already online in South London. Uber claims the response to the ID check was sent from the iPhone at around 11:55 pm that evening.

The next day, Uber informed him that his account had been 'flagged for suspicious application activity' and that his account would now be suspended while 'a specialised team reviews this.' Sometime later, Uber permanently dismissed Aweso via text saying that they had 'found evidence indicating fraudulent activity' on his account. Uber then alleged that he was sharing access to his account and in doing so had breached terms and conditions. The next month, Transport for London immediately revoked Aweso's license on the grounds that he could no longer be found to be 'fit and proper' to hold a public license, based on his dismissal from Uber.

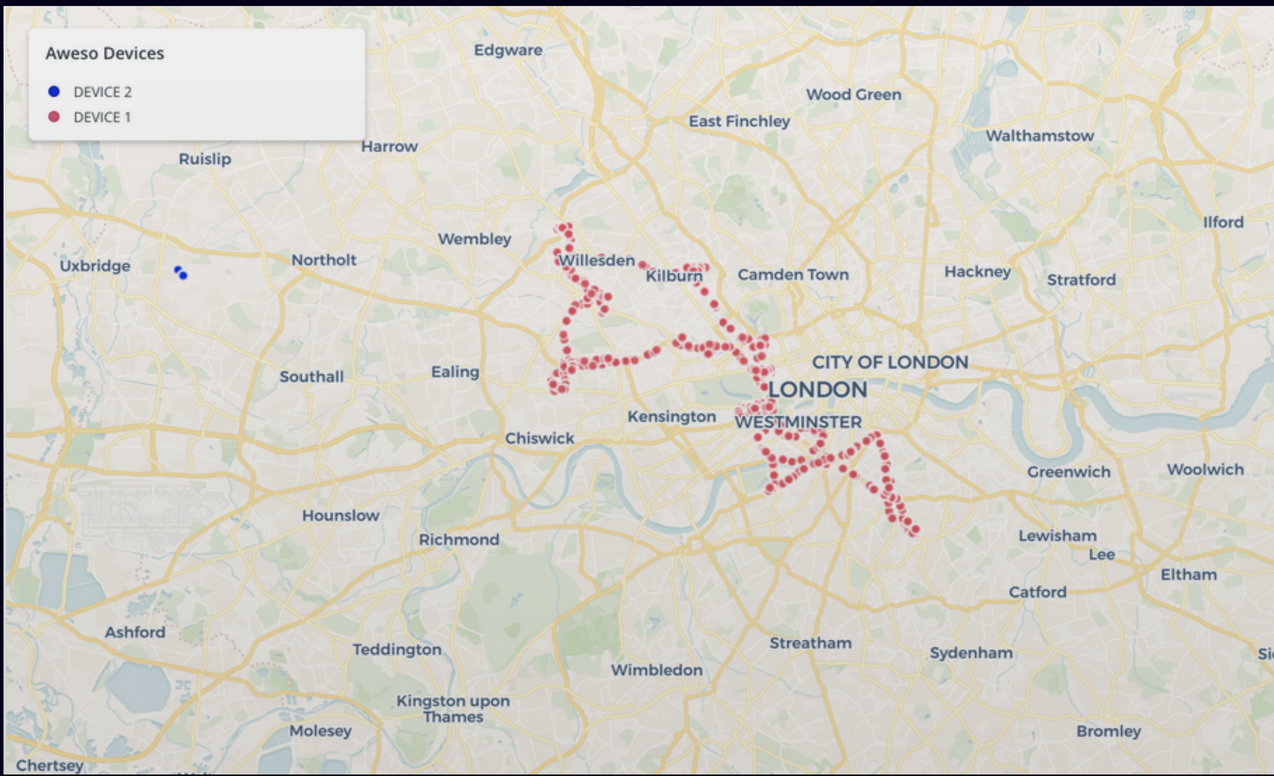
Worker Info Exchange assisted Aweso in making a subject access request and analysing the data received. One file called 'Driver Detailed Device Data' records at least some of the data streaming from devices to Uber in real time. From this file we could see as much as 230 rows of data per minute being recorded by Uber from devices. The data Uber collected from Aweso's devices included geo-location, battery level, speed, course heading, IMEI number etc.

The data showed that the device in Uxbridge had never been logged in for work on that day because a field entitled 'driver_online' showed the iPhone as 'FALSE' at all times that day including the time it was recorded at Uxbridge. This is proof that the device was not being shared for work with others as alleged by Uber and Transport for London. Uber failed to provide access to personal data processed in both RTID checks including the photos collected. The 'Detailed Device Data' shows no record of any further activity for the iPhone after 8:03:43 pm. We saw no data evidence of device activity at 11:55 pm when Uber said it received a response to the earlier issued ID check.

The experience of Pa and Aweso was very prevalent during the past year and made up a significant volume of casework handled by Worker Info Exchange and the App Drivers & Couriers Union. In London, Transport for London tended to immediately revoke the licenses of drivers who were reported to have failed Uber's RTID checks despite the obvious problems with the system. There are often reasonable explanations for multiple device use which are automatically classified as fraud. Uber's own privacy policy indicates that where a device has the app open in the background or foreground, even if not online and ready to accept fares. It is worth noting that under Article 6 of the proposed new EU Directive on platform work the surveillance of and collection of any personal data while the platform worker is not offering or performing platform work (as in this case) would be banned.

In more than a dozen cases where we supported driver's appealing their revocations at the Magistrates Court, every appeal was upheld and TfL were ordered to reinstate the licenses. Uber commented that in cases like these, "human reviewers may still decide to deactivate the account, even if the driver has passed the photo verification."

Worker Info Exchange, Big Brother Watch and the App Drivers & Couriers Union wrote a joint letter to the Mayor of London to raise our concerns about Transport for London's reliance on flawed evidence from Uber in making a revocation decision and demanded that, as Chair of Transport for London's board, that he order a review of all such wrongful revocations. To date, neither the Mayor nor TfL have responded.

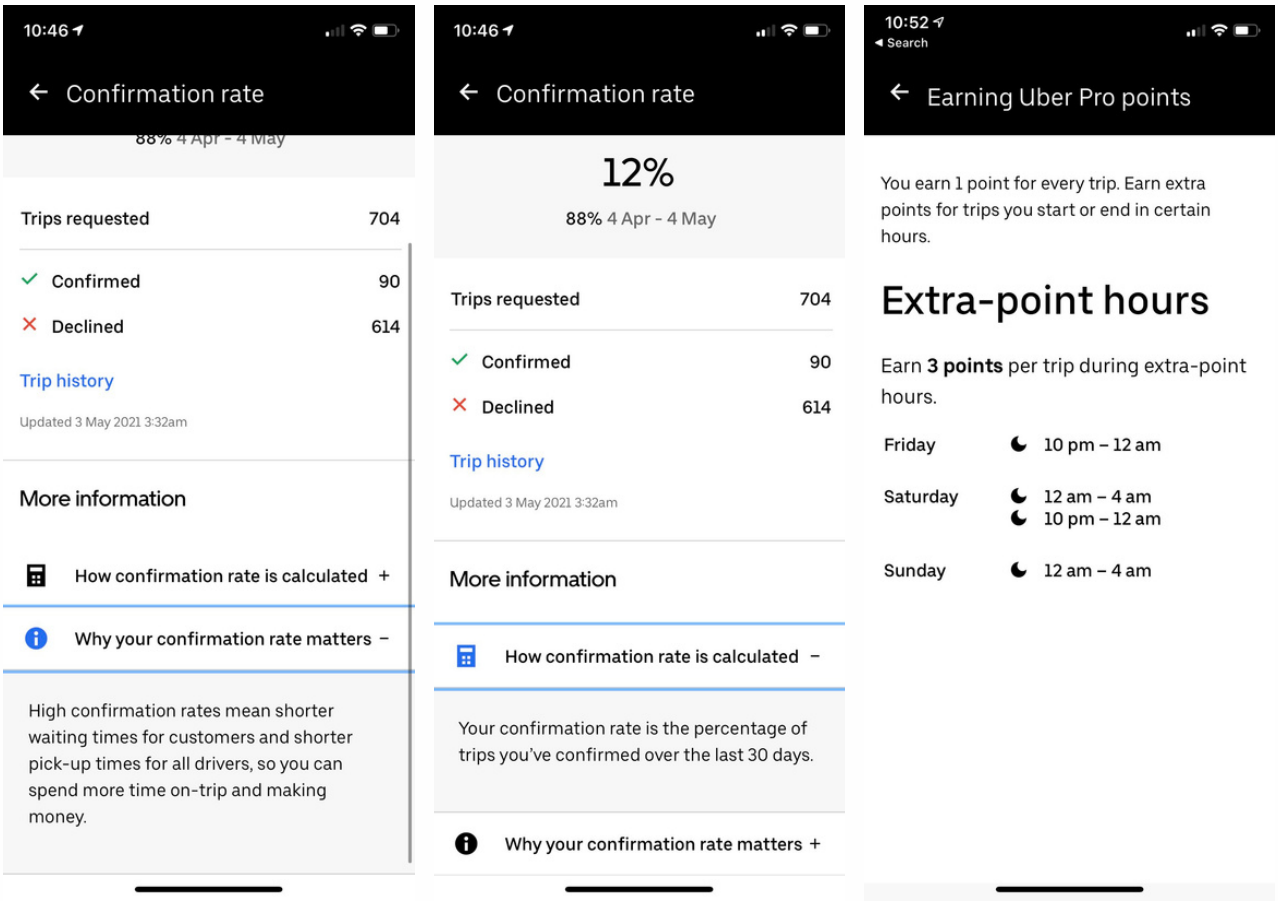


altitude	course	speed	horizontal_accuracy	gps_time	vertical_accu	driver_online	city_name	city_name_id	os	os_versio	model	language	version	carrier
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	-1	65	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE	london	18	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE		\N	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE	london	18	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE
\N	\N	0	32.43388632	11/09/2020 20:02	\N	FALSE	london	18	ios	13.7	iPhone12,1	en_GB	4.266.10002	EE

Opaque Performance Management

The opacity of platforms inhibits understanding of how algorithmic control might be integrated across the span of critical processes and over time. For example, workers have not been provided the transparency they are legally entitled to in order to understand how performance profiling links to the quality and quantity of the work offered, as well as the expected yields for such work. In the case of Ola, we have some knowledge of the data categories they collect and process in their work allocation systems - such as fraud probability scores, earning profiles, booking acceptance and cancellation history, among others - however this does not reveal the different weightings applied to these variables, nor the logic of processing.

Uber has long maintained that its matching system is solely determined by location, despite its own "Partner-Driver" interface suggesting otherwise. Uber's Pro programme (which drivers are automatically enrolled into so they can be incentivised to meet performance goals in exchange for benefits and rewards) informs drivers in vague language that "higher confirmation rates mean shorter waiting times for customers and shorter pick-up times for all drivers" loosely alluding to the fact that declining jobs may result in fewer job offers.



Uber has only recently offered more transparency on the matching system through an update to their privacy policy which states, "Users can be matched based on availability, proximity, and other factors such as likelihood to accept a trip based on their past behavior or preferences." We made a freedom of information request to TfL, inquiring about what updates Uber had provided on its matching system, as it is obliged to do when making changes to its operating model. This returned no results, further highlighting the obfuscation of its algorithmic management practices and the absence of regulatory oversight. However, despite this recently updated description of the matching system, Uber strongly contested the use of past behaviour or preferences for work allocation in a statement they provided about our report: "To be clear and specific: Uber does not use individual behavior or performance when matching drivers with riders. It is based on location together with road and traffic conditions, rather than based on who they are, how they behave or perform."

These uncertainties on the variables determining work allocation also raise important questions about the quality of jobs offered to drivers. Are drivers with high job acceptance rates offered trips of longer length and duration, resulting in higher pay, on the basis of similar profiling? In recent years, Uber has replaced time and distance based pricing for customers with a fixed pricing model in which an upfront price is accepted at the start of a trip. Uber states, "upfront pricing is dynamic, which means the price is worked out in real time to help balance supply and demand." How these systems interact and whether and how algorithmic pricing is brought together with work allocation is a sensitive issue about which little is still known. Even if this is not the intention of platforms, how can we be reassured that past driver preferences for higher or lower yielding work won't result in them being offered more of the same, producing an auction type bidding for differently priced trips?

With the inconsistent narratives provided on these systems, and the concerns already raised about the discriminatory outcomes of using dynamic pricing systems on passengers, the prospect that drivers could also be subject to such pricing mechanisms is an issue that requires close inspection. There are serious ethical issues here if operators are offering lower prices to vulnerable workers based on profiling which predicts their willingness to accept work at different price points. In response to this question, Uber again denied any connection between user profiling and individual driver pay or passenger pricing. In their statement, Uber said: "suggestions that Uber offers variable pricing based on user-profiling is completely unfounded and factually incorrect."

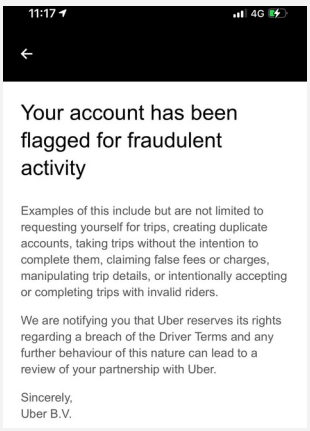
In the UK, such practices appear to run contrary to the provisions of Section 1 of the Employment Rights Act which entitles workers to receive from their employer a clear statement of the terms of conditions of their work including rates of pay.

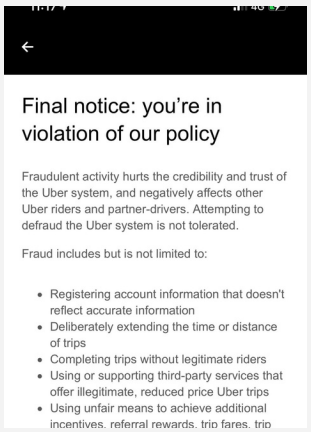
Case Study

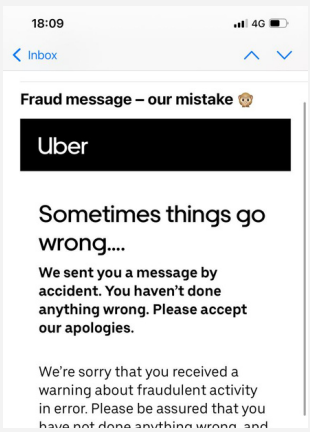
Algorithmic Control

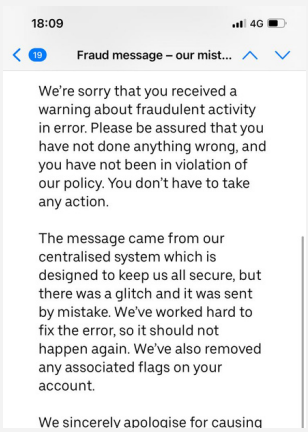
Watch interview

Uber routinely sends drivers messages when they are flagged by its fraud detection systems to warn them that they may lose their job if they continue whatever behaviour is triggering the system. The messages contain a non-exhaustive list of the potential triggers, but do not provide a reason specific to the driver that is being accused of fraud. When Alexandru received the second and final one of these messages, knowing another flag would result in dismissal, he decided to call the driver support team to get further details on why he was triggering the anti-fraud system and what he could do to avoid it. Through the call, Alexandru and the support agent discussed a variety of situations that may have caused his trips to appear irregular, revealing the limited ability support teams have in deciphering the indications made by the system. Three months after this call, Uber sent an apology message stating that he had been sent the warnings in error.





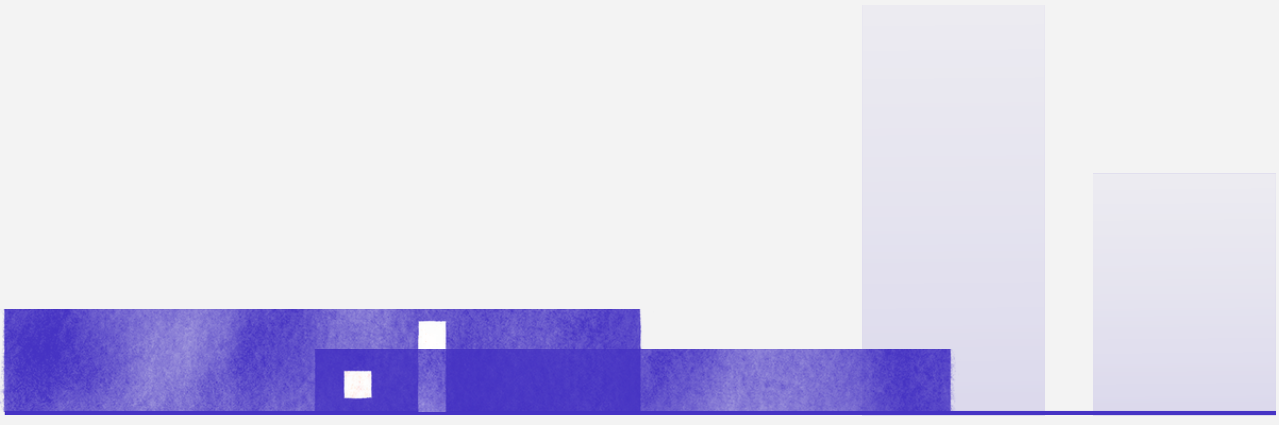




While the conversation is enlightening in terms of understanding the dilemmas drivers face when company policy and passenger demands diverge, of particular interest to us was the discussion (25 minutes into the call) concerning a detour Alexandru took due to roadworks, as well as his low job acceptance rates as potential causes of his detection by the anti-fraud system. Following the Supreme Court ruling that classified Uber drivers as workers earlier this year, Uber claimed to have made significant changes to its platform such as offering transparency of price and destination, as well as removing punitive measures for refusing jobs, in a bid to argue that the Supreme Court ruling did not apply to current Uber drivers.

Alexandru's experience on the platform runs counter to this narrative, as it becomes apparent that he is likely being flagged for deviating from route (despite the fact that Uber is now operating a fixed price model, meaning drivers make such routing changes at their own expense) and not accepting enough of the work offered to him on the platform. This call makes it undeniably clear that in practice, drivers are as tightly controlled by Uber as before.

In addition to these management practices, the Pro programme mentioned above is another tool that Uber uses to exercise control over its workforce, while evading the legal obligations that may be associated with such control. For example, by tying rewards culminating from maintaining a high rating to third party companies or presenting participation in pricing benefits as purely optional through behavioural nudging, Uber creates the illusion of letting drivers operate with complete independence and flexibility. The drivers' supposed voluntary engagement with these programmes result in the relinquishing of rights proceeding from having an employment relationship.



11:17 4G

Your account has been flagged for fraudulent activity

Examples of this include but are not limited to requesting yourself for trips, creating duplicate accounts, taking trips without the intention to complete them, claiming false fees or charges, manipulating trip details, or intentionally accepting or completing trips with invalid riders.

We are notifying you that Uber reserves its rights regarding a breach of the Driver Terms and any further behaviour of this nature can lead to a review of your partnership with Uber.

Sincerely,
Uber B.V.

11:17 4G

Final notice: you're in violation of our policy

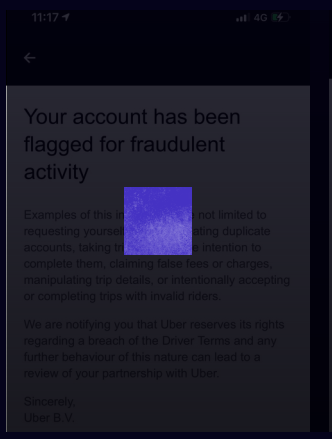
Fraudulent activity hurts the credibility and trust of the Uber system, and negatively affects other Uber riders and partner-drivers. Attempting to defraud the Uber system is not tolerated.

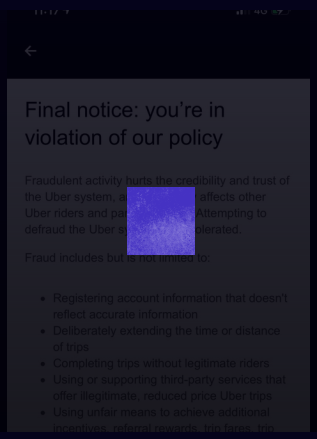
Fraud includes but is not limited to:

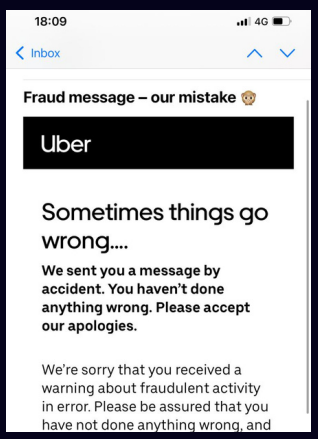
- Registering account information that doesn't reflect accurate information
- Deliberately extending the time or distance of trips
- Completing trips without legitimate riders
- Using or supporting third-party services that offer illegitimate, reduced price Uber trips
- Using unfair means to achieve additional incentives, referral rewards, trip fares, trip adjustments, promotional fares, or high ratings.

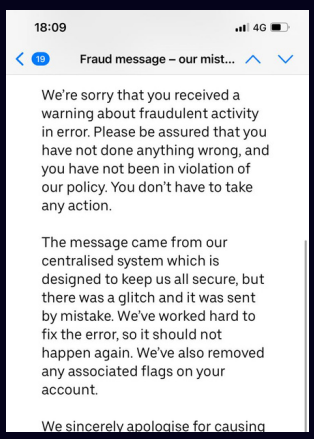
Your account has had excessive amounts of fraudulent trips and you are now required to explain the account behaviors of the past 2 weeks before being reactivated.

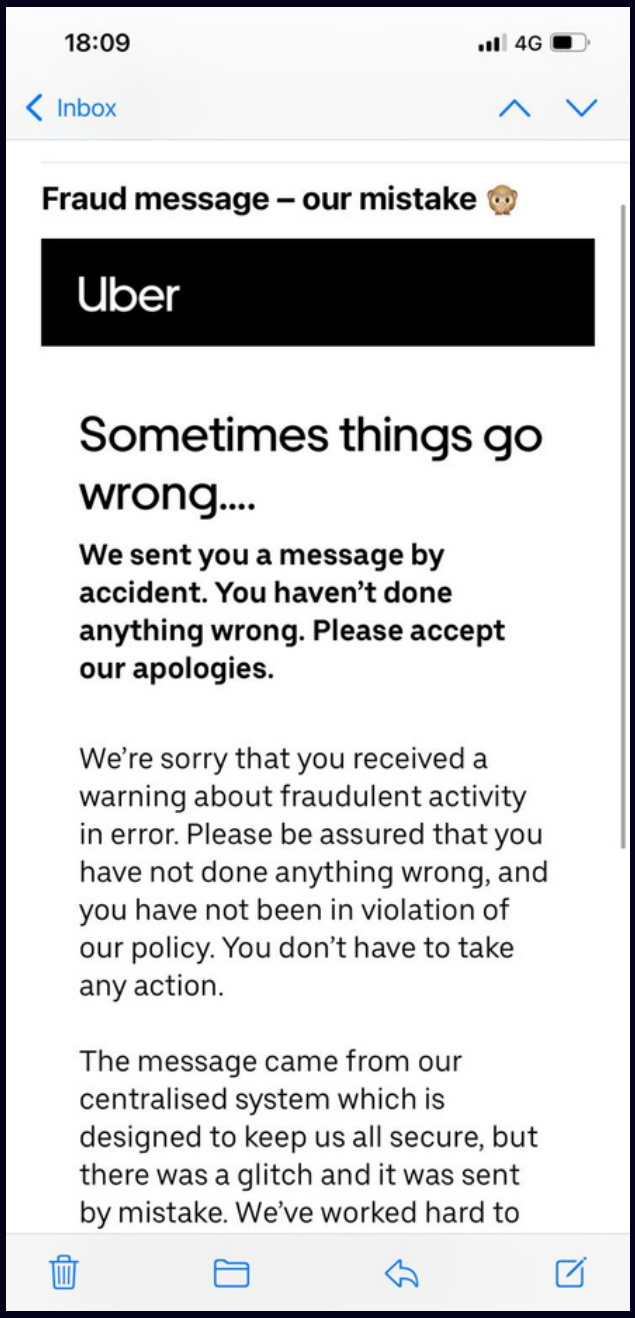
Yours Sincerely,
Uber B.V.

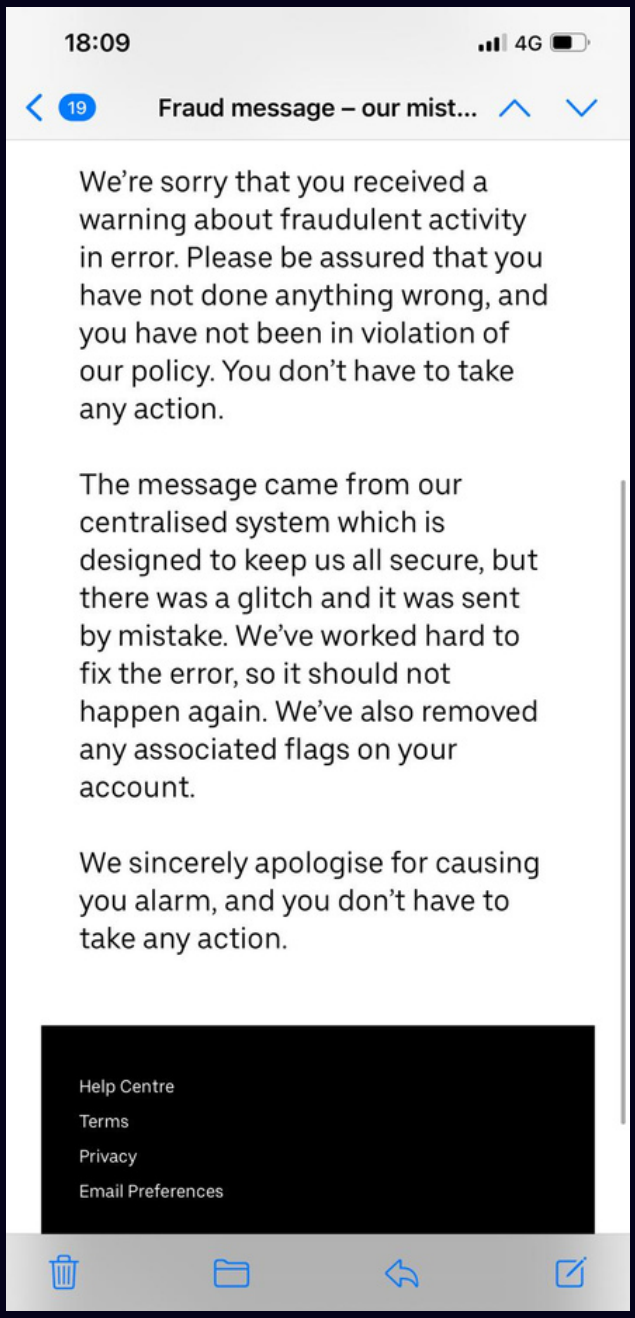


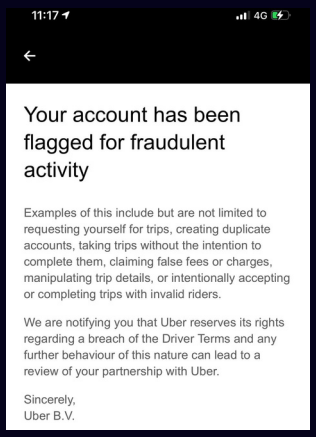


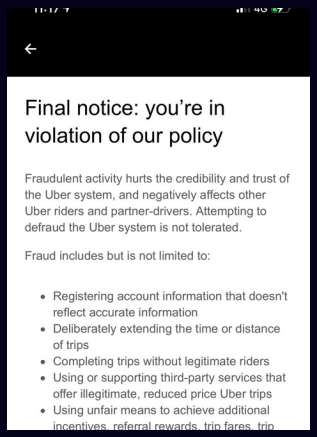


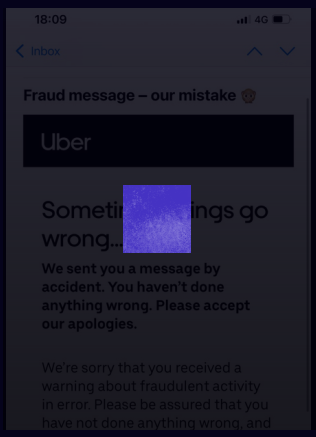


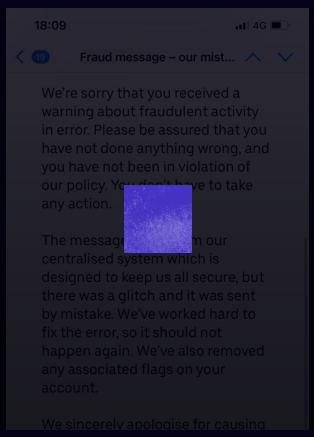

18:09
4G
Inbox
Fraud message – our mistake 🐵
Uber
Sometimes things go wrong....
We sent you a message by accident. You haven't done anything wrong. Please accept our apologies.
We're sorry that you received a warning about fraudulent activity in error. Please be assured that you have not done anything wrong, and you have not been in violation of our policy. You don't have to take any action.
The message came from our centralised system which is designed to keep us all secure, but there was a glitch and it was sent by mistake. We've worked hard to


18:09
4G
19
Fraud message – our mist...
We're sorry that you received a warning about fraudulent activity in error. Please be assured that you have not done anything wrong, and you have not been in violation of our policy. You don't have to take any action.
The message came from our centralised system which is designed to keep us all secure, but there was a glitch and it was sent by mistake. We've worked hard to fix the error, so it should not happen again. We've also removed any associated flags on your account.
We sincerely apologise for causing you alarm, and you don't have to take any action.
Help Centre
Terms
Privacy
Email Preferences


11:17
4G
Your account has been flagged for fraudulent activity
Examples of this include but are not limited to requesting yourself for trips, creating duplicate accounts, taking trips without the intention to complete them, claiming false fees or charges, manipulating trip details, or intentionally accepting or completing trips with invalid riders.
We are notifying you that Uber reserves its rights regarding a breach of the Driver Terms and any further behaviour of this nature can lead to a review of your partnership with Uber.
Sincerely,
Uber B.V.


Final notice: you're in violation of our policy
Fraudulent activity hurts the credibility and trust of the Uber system, and negatively affects other Uber riders and partner-drivers. Attempting to defraud the Uber system is not tolerated.
Fraud includes but is not limited to:
Registering account information that doesn't reflect accurate information
Deliberately extending the time or distance of trips
Completing trips without legitimate riders
Using or supporting third-party services that offer illegitimate, reduced price Uber trips
Using unfair means to achieve additional


18:09
Fraud message – our mistake
Uber
We sent you a message by accident. You haven't done anything wrong. Please accept our apologies.


18:09
Fraud message – our mist...

Expansion of Law Enforcement Infrastructure

There is also evidence that platforms have increasingly become an attractive source of intelligence for police and security services. In a witness statement presented in evidence in September 2020 at Uber's licensing appeal at the Westminster Magistrates Court, Uber's General Manager from the UK and Western Europe Jamie Heywood attested to an increasingly close relationship with the police and security services. These include the National Counter Terrorism Policing Network, SO15 - the Counter Terrorism Command of the Metropolitan Police Service, the National Police Chiefs Council (NPCC), the College of Policing, the National Crime Agency and the British Transport Police. One area of cooperation has been on the problem of so-called County Lines transportation of drugs. Quoting Detective Inspector Stuart Liddell of the NPCC, Heywood testified to a maturing relationship based on sophisticated levels of intelligence sharing:

> "I am encouraged by the engagement displayed by Uber regarding this matter and further work is planned [in 2020] to build on the work so far. This will focus on more intricate aspects of the County Lines, the flow of information and intelligence and the strengthening of the relationship between the National County Lines Coordination Centre."

Indeed, the NPCC lobbied Transport for London Commissioner Mike Brown in support of Uber's license appeal. Chief Constable Mark Collins even went so far as to suggest that a decision to deny Uber their license might have a negative impact on UK policing.

> "Hopefully, this letter outlines the negative impact on UK policing should police not be able to access the data and information I have described."

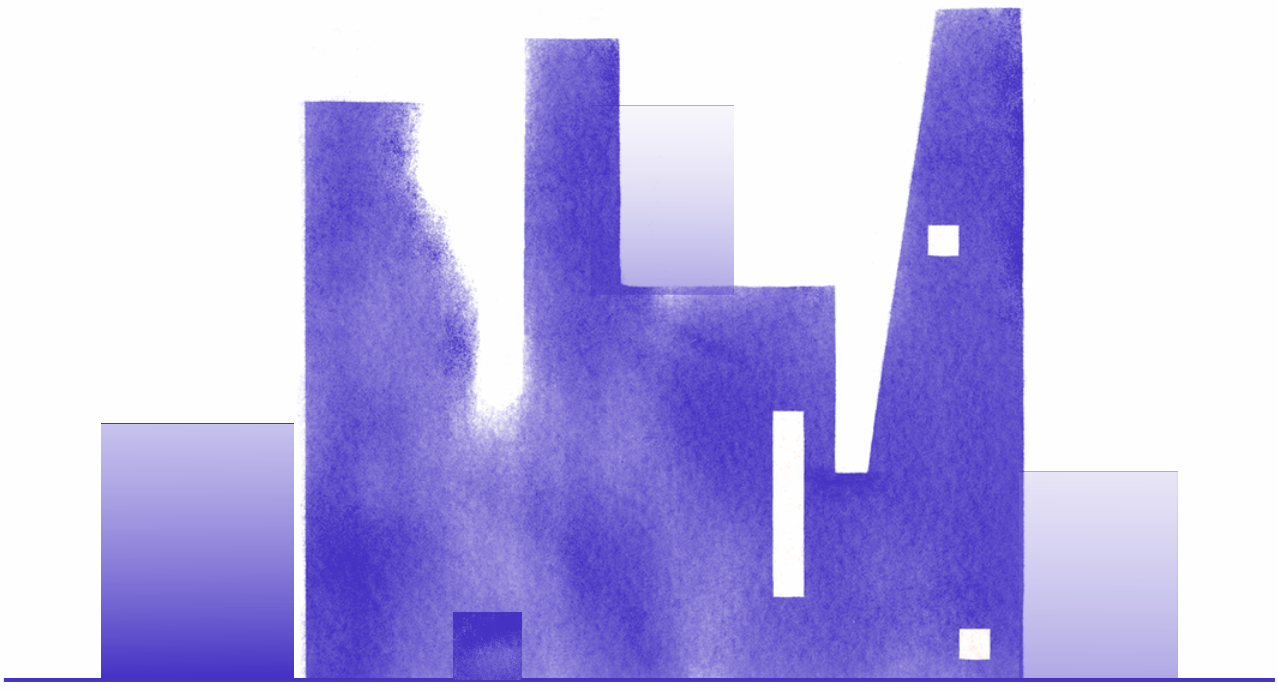
Heywood also testified that Collins had claimed that the Metropolitan Police Service alone made over 2,000 requests for data to Uber each year. This is a relatively high number of requests considering that, according to Uber's own Transparency Report, in 2020 all US law enforcement authorities combined made just under 5,000 data requests and all Canadian law enforcement authorities combined made just 411 such requests.

It is likely that Uber management feels pressure to cooperate with police intelligence gathering initiatives, particularly in light of the decision of Transport for London to refuse renewal of their license twice. This is because section 17 of the Crime and Disorder Act 1998 places a direct responsibility on licensing authorities to prevent crime and disorder in their area. This sets up a requirement for licensing authorities such as Transport for London to establish Crime and Disorder Reduction Partnerships (CDRP) to which transport operators such as Uber are expected to participate in.

In the Department for Transport's statutory guidance to licensing authorities, the government reinforces the expectation of intelligence sharing between the police, licensing authorities and transport operators such as Uber:

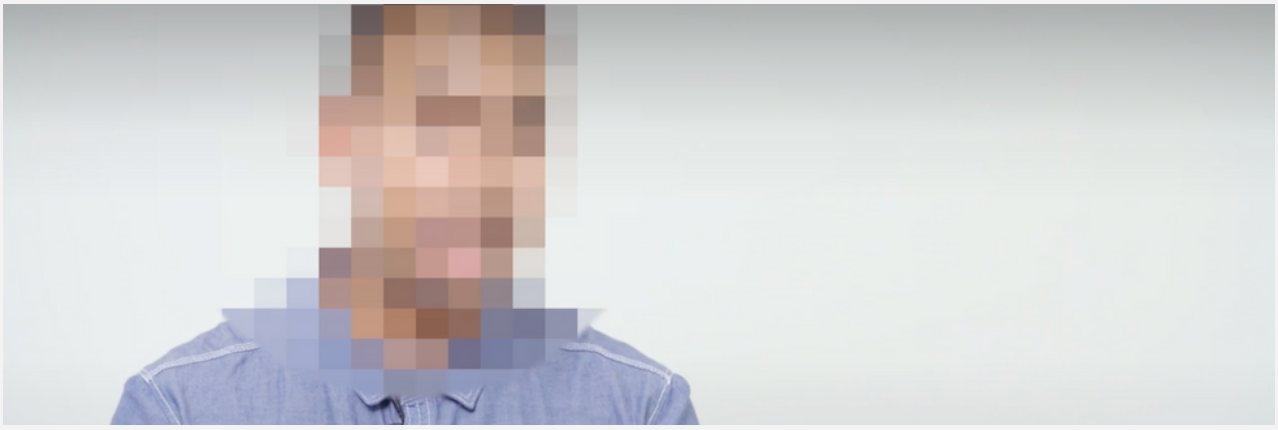
> "Increasing the awareness among police forces of the value licensing authorities place on the information received, particularly on non conviction intelligence, will assist furthering these relationships and reinforce the benefits of greater sharing of information. This relationship can be mutually beneficial, assisting the police to prevent crime. The police can gain valuable intelligence from drivers and operators..."

While such relationships have significant importance for community level crime control, it seems little regard has been paid to the risk to civil liberties of relatively easy access to rich personal data of drivers and passengers as collected and stored by platforms.



Case Study

Intelligence Sharing with Law Enforcement



Watch interview

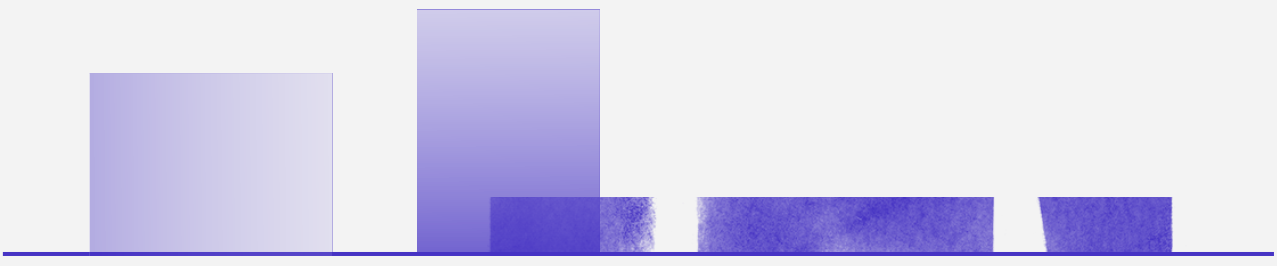
Another worker who approached us for help was an Uber driver who was wrongly suspended from the Uber platform for seven weeks, incurring a loss of nearly £5000, following an intelligence request made by the police. In 2019, the driver received a message from Uber stating that he was temporarily suspended due to an ongoing investigation. He was given neither a reason, nor a timeframe for his suspension. In fact he was expressly told not to contact Uber while they carried out the investigation. Seven weeks later, he received a call informing him that he could now work.

Two years later, a license renewal application the driver made to TfL (which includes an enhanced Disclosure and Barring Service check) revealed the reason for suspension, when TfL questioned him about supplying drugs in 2019 and threatened to take his license away. Shocked by the revelation, the driver demanded a crime reference number, and made further inquiries not just with TfL, but also the Metropolitan Police.

We assisted the driver in making subject access requests and complaints to Uber, TfL and the police. Uber failed to fulfil the request (the driver was informed that his request was passed on to a specialist team but received no further response) however, TfL's response uncovered an extensive chain of emails between various officials as they attempted to identify the source of the intelligence request. Uber claimed they had been approached by the police while the police failed to locate any record or evidence of investigating the driver. Eventually, Uber named the officer who had made the intelligence request but when TfL sought details about the case, the OIC claimed he had no recollection of the driver in question.

The complaint the driver made to the Metropolitan Police was finally answered in October 2021 and concluded that the driver had never been identified as a suspect:

> "Officers were tasked with identifying a suspect in relation to a serious crime. Officers had been passed the name of a person of interest. I can confirm this was NOT you. A data protection form was submitted on 20 February 2019 to Uber with this named suspect details. I am not at liberty to disclose any further details about this.
>
> "At no stage did your name feature in this research enquiry made with Uber. The officer did NOT approach Uber looking for any information connected to you. As a result of our enquiry, Uber provided the police with your details. Once the information was received back from Uber and they gave us your name, we knew you were NOT linked to our investigation and no further action was taken and you were excluded from any further enquiries."
>
> "The officer has not breached any professional standards nor acted outside of their role as a police officer or abused their power. Your name was not the purpose of the request and at no point did we tell Uber that you were a person of interest."
>
> "Uber should perhaps explain how they suspend someone who was not the subject of the original request and also why, after 10 days, you were not automatically reinstated into the app and able to carry on working."



Dear Team

Re: 195283

We have been notified by Uber about the suspension of the driver [redacted] due to being under investigation by the police for drug supply. The police informed Uber about the investigation on 12 March 2019.

Could you please obtain an update regarding this investigation?

[redacted] I cannot find anything that would suggest that this is a Met Crime. Can you see where Uber got this information from.

[redacted]

[redacted]

On 12 March 2019, Uber's Law Enforcement Response Team were contacted concerning [redacted] from Officer [redacted]. The message stated that [redacted] was a person of interest in relation to the supply of drugs. Officer [redacted] contact details are [redacted] and [redacted]@met.pnn.police.uk.

An Uber support representative contacted [redacted] regarding the investigation. [redacted] was advised that he may be a part of a police investigation, however he was not made aware of the details of the investigation. [redacted] was asked if the police had been in touch with him, to which he advised they had not been. Mr [redacted] advised he had no idea as to why the police would be investigating him. Mr [redacted] advised he could not think of any reasons concerning riders or in general as to why the police would be investigating him.

On 20 April 2019, LERT was advised by Law Enforcement that [redacted] was no longer a safety concern, therefore his access to the app was reinstated.

Re: ISA disclosure update - [redacted]

Having shared the above driver's and OIC's details with TPHPT we have been informed that the police officer and incident is not recorded on the PNC. TPHPT have advised to make contact with Operator and obtain further details (see below).

Intel will contact Uber.

Regards

[redacted] Unfortunately [redacted]s the officer who put the request in on behalf of the OIC and is unable to gain access to see who that was. Can you return to Uber and see if they have any other details that may identify who the OIC is.

[redacted]

It is alleged that the driver had been under police investigation, relating to the possession of drugs which had resulted in the driverâ€™s suspension on 13/03/2020.

We have since shared this information with the Metropolitan Police who were unable to locate the incident or individual on their data base.

In order review the driverâ€™s fitness to continue to be licensed please can you confirm the name of the police officer (OIC), the police force and crime reference number.

Aisling O. (Uber)

Jan 15, 2021, 9:14 GMT

Hi [redacted],

Thank you for reaching back out to us in relation to this matter. Apologies for any inconvenience caused here. However, we wish to advise you that our reasoning for reaching out to the police first in this instance is due to your request relating to a covert police investigation.

We hope that this helps to clarify matters and we believe that the officer should be in contact with yourselves in due course. However, if you continue to experience difficulties in relation to progressing with this, please do not hesitate to let us know and we will be happy to do what we can to assist.

From: [redacted] - Specialist Crime South [redacted]@met.police.uk>
Sent: 15 May 2021 17:28
To: [redacted] <[redacted]-[redacted]@met.police.uk>
Subject: ISA/11/2019

Dear Sergeant [redacted],

I've searched on his name in my inbox and I cannot find anything that would help I'm afraid.

I have also searched the DPA/all material folders for the operations that were running at around that time and no trace either

I have also searched for his name on the [redacted] server on [redacted] and also on [redacted] and (uber) as usually the DPA would be attached to a Crimint log where a search as described would find it.

Can Uber provide anything else? An email chain perhaps?

The name means nothing to me I'm afraid, was an operation name given to Uber?

Thanks

Morning [redacted]

You have been named as the possible OIC for the below subject who is / was a licensed PHV driver.

I cannot find any Cris pertaining to the below which may well be restricted and he is no trace on PNC so can I ask firstly if you remember this chap and if so can you please provide me with;

Cris number... and

- was the driver spoken to
- was the driver arrested, if so what date
- if the driver was eliminated from enquiries, why

Thanks

[redacted]

This is an aged one but wanted to get some things clarified as I don't believe this was chased up any further.

In your last response you asked for further details of the OIC (pasted below), Uber have confirmed the OIC as [redacted].

Could you please confirm what investigation took place in regards to drug supply. If possible can you please confirm the following:

- was the driver spoken to
- was the driver arrested, if so what date
- if the driver was eliminated from enquiries, why

Good afternoon,

We received the following from Uber on 13 March 2019.

On 12 March 2019, our Law Enforcement Response Team received notification from the Metropolitan Police that [redacted] under investigation for drugs supply. The Police have asked for [redacted] to not be notified of their investigation for the next 14 days (starting 12 March 2019). Mr [redacted] access to the Uber application will remain disabled while this matter is being investigated.

Could you please provide contact details of who in the Metropolitan Police contacted you initially, and forward any updated information you may have either from the police or your investigation.

[redacted] (TPH)
Jan 4, 2021, 15:52 GMT

Dear Sir/Madam,

In regards to driver suspension notification for driver number [redacted]

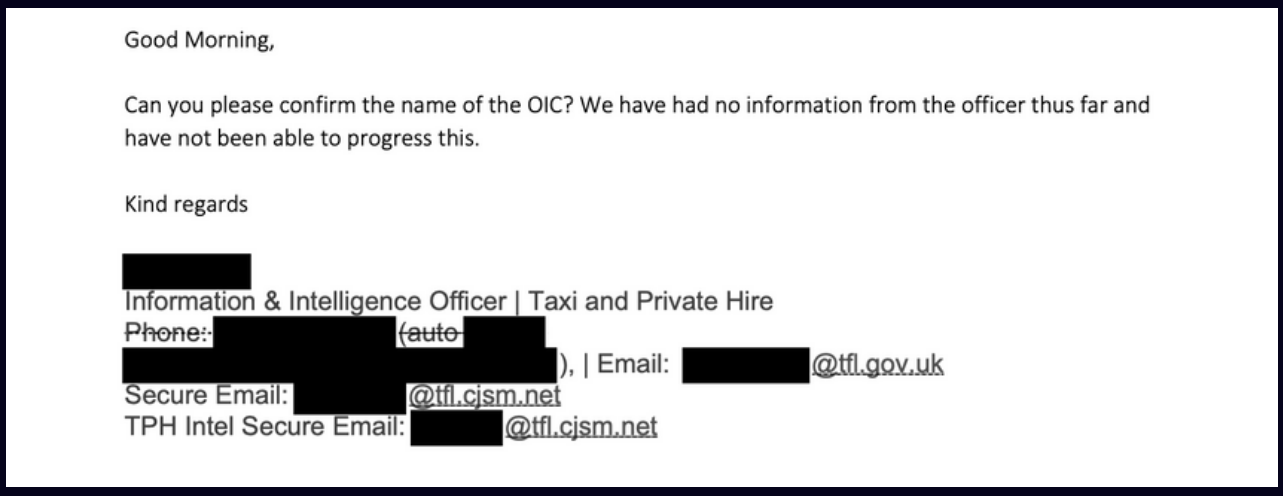
We had been made aware that on 19/03/2020 Uber had been contacted by the police regarding the above driver reference.

It is alleged that the driver had been under police investigation, relating to the possession of drugs which had resulted in the driver's suspension on 13/03/2020.

We have since shared this information with the Metropolitan Police who were unable to locate the incident or individual on their data base.

In order review the driver's fitness to continue to be licensed please can you confirm the name of the police officer (OIC), the police force and crime reference number.

Regards



Good Morning,

Can you please confirm the name of the OIC? We have had no information from the officer thus far and have not been able to progress this.

Kind regards

[redacted]
Information & Intelligence Officer | Taxi and Private Hire
~~Phone:~~ [redacted] ~~(auto~~ [redacted]), | Email: [redacted]@tfl.gov.uk
Secure Email: [redacted]@tfl.cjsm.net
TPH Intel Secure Email: [redacted]@tfl.cjsm.net

[redacted] (Uber)

Jan 6, 2021, 14:42 GMT

Hi [redacted]

Thank you for reaching out regarding the suspension notification for [redacted] which was issued on 13 March 2019.

We have looked into this and can confirm that the officer associated with this report has been asked to make contact with TfL or the Taxi and Private Hire Unit directly.

I have reviewed documentation produced from February 2019 at the time the alleged disclosure was made to Uber and that are linked to this complaint. I have spoken to the officer whose name has been linked to your concerns.

Officers were tasked with identifying a suspect in relation to a serious crime. Officers had been passed the name of a person of interest. I can confirm this was **NOT** you. A data protection form was submitted on 20 February 2019 to Uber with this named suspect details. I am not at liberty to disclose any further details about this.

At no stage did your name feature in this research enquiry made with Uber. The officer did **NOT** approach Uber looking for any information connected to you. As a result of our enquiry, Uber provided the police with your details. Once the information was received back from Uber and they gave us your name, we knew you were **NOT** linked to our investigation and no further action was taken and you were excluded from any further enquiries.

I can confirm that nothing more since that date has been carried out where you have come to notice. I have reviewed this data protection document and the reason it was submitted and I can confirm it was submitted correctly and within the law. The officer has not breached any professional standards nor acted outside of their role as a police officer or abused their power. Your name was not the purpose of the request and at no point did we tell Uber that you were a person of interest.

I have spoken to Uber to find out why you were suspended from driving. Their policy is to suspend from the app any person who is linked to any form of information requests, complaints from passengers or other such like. After 10 days, if Uber do not receive further information to follow up any concerns to keep a driver suspended, they relinquish the suspension and allow access again to the app and a driver can operate again. Uber failed to adhere to the request made by police by making their own assumptions and conclusions and by suspending you from driving.

Uber should perhaps explain how they suspend someone who was not the subject of the original request and also why, after 10 days, you were not automatically reinstated into the app and able to carry on working.

I have also spoken to Uber and asked them to remove any notes against your name, again to show you are not under police investigation and not a drug dealer. This was done on 9th August 2021 and your Uber file has been endorsed accordingly.

One of the requests you made to me was for your name to be fully cleared with TFL. This is something I am I the process of doing. I wrote to them on 10th August 2021 and asked for any details they have linking you to any wrong doings connected to this incident or showing that you are a drug dealer to be removed. I chased them up again on 9th September 2021 and I am yet to receive a definitive answer.

As far as the compensation element of your complaint, I believe this is something your legal team should take up with Uber. I don't believe the Metropolitan Police is responsible for this as all of our checks were carried out lawfully and within the officer's role as an investigator and it was Uber who disclosed your details to us and also failed to reinstate you after their automatic 10 day period.

"It is extremely worrying that workers in the gig economy risk having their right to access their data at work so restricted and protections from automated decisions such as performance profiling, work allocation and even robo-firings extinguished.

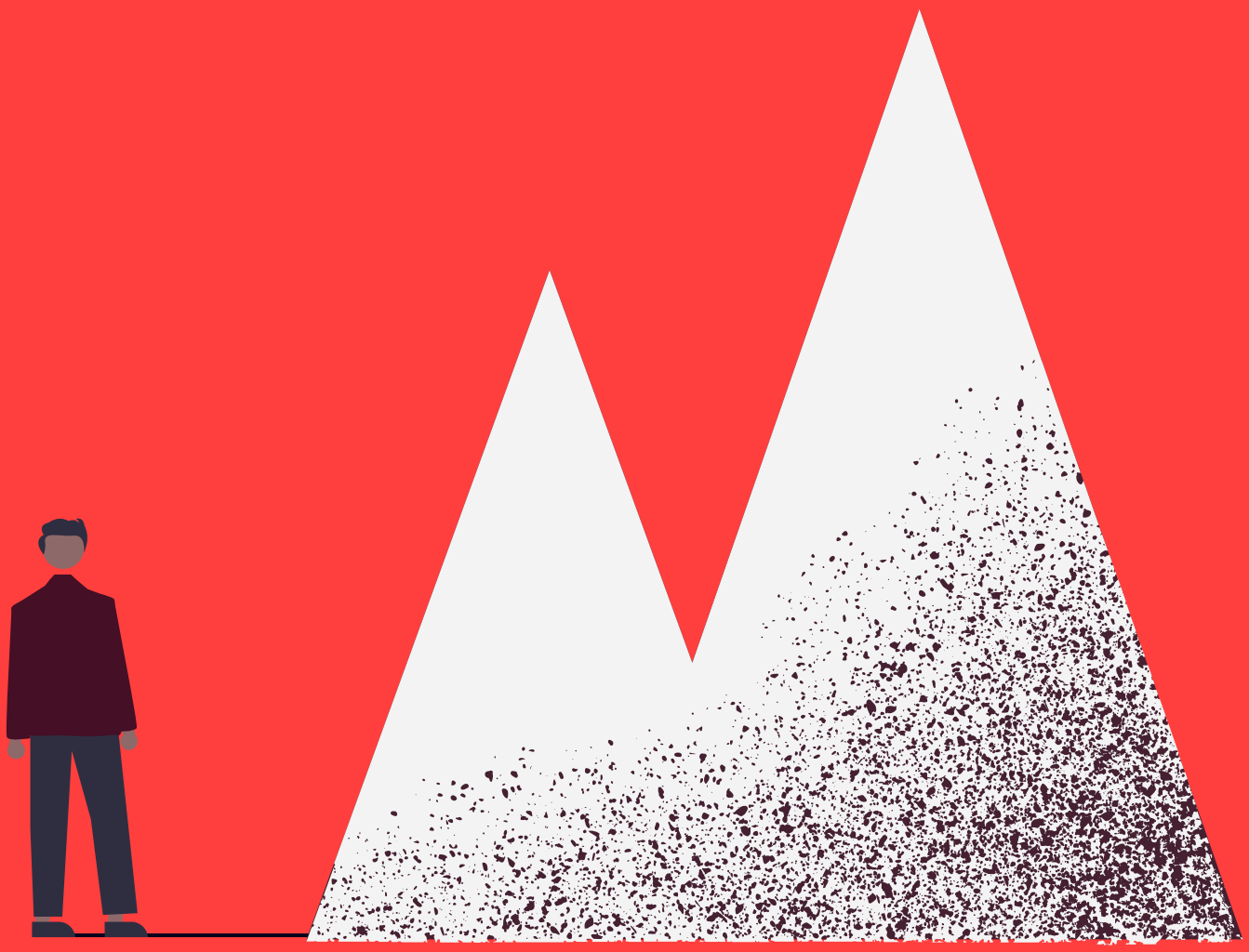
This abuse serves to underline why we have to have a new deal for all working people that delivers a single status of employment for all workers save for the genuinely self-employed, with full rights and protections from day one.

Clearly companies will fully exploit the opportunities that bogus self-employment affords them to abuse and exploit their work force, unless that opportunity is closed off by legislation to deliver fundamental employment rights and protections for all."

Andy McDonald, MP

Part II

Exercising Data Rights at Work: Access

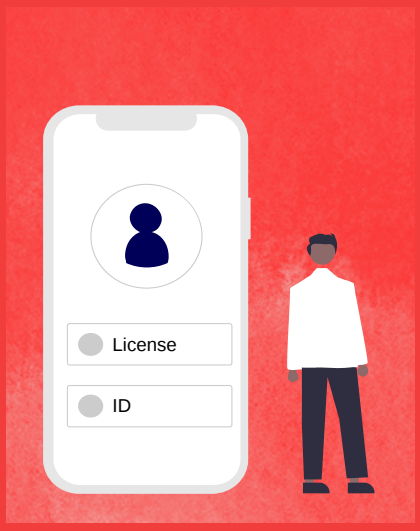


Overview

Employment law does not have the necessary provisions to fully protect workers from the unfair practices stemming from algorithmic management. However, individuals have rights under the GDPR that can protect their interests within employment contexts. In supporting workers, we invoke their rights as defined by Article 15, 20 and 22, which give them the right to access personal data, the right to data portability, as well as the right to be informed about automated decision-making and the logic of processing.

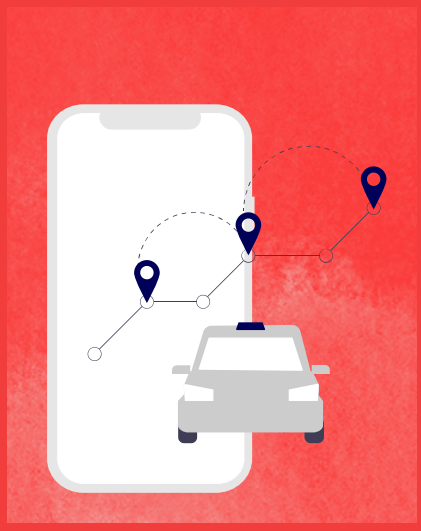
Article 22	Data subjects cannot be subject to decisions with legal (or similarly significant) effects, based solely on the automated processing of data. [If the data controller processes data with the data subject's explicit consent, or for the performance of a contract with them, the data subject has the right to obtain human intervention, to express their point of view, and to contest the decision].
Article 15	Data subjects have the right to receive a copy of their personal data, along with supplementary information such as the purposes for processing data, information about who the data may be shared with, the duration of processing etc.
Article 20	Data subjects have the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. They also have the right to transmit ('port') the data to another controller. Where feasible, they may ask for the data to be transmitted directly from one controller to another.

While platforms do make data downloads available to workers, these frequently omit the data categories most conducive and necessary for interrogating the conditions of work (such as fairness of pay, job allocation and utilisation, as listed above.) In our aspiration to expand the scope of data made available to workers, we make specific subject access & portability requests that cover the full range of data gig platforms collect from them. In these requests, we seek to obtain three different types of data:



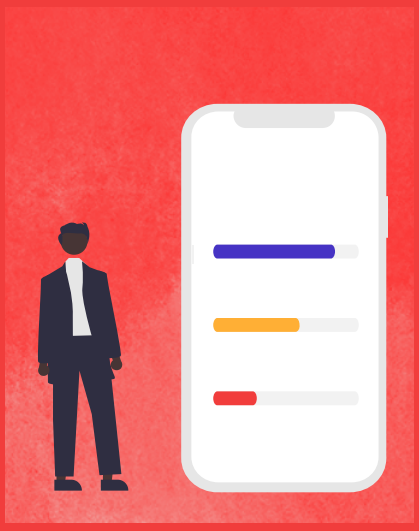
Input data

Provided by the workers themselves



Observed data

Based on workers' use of platforms (i.e. raw measurement and surveillance data such as location data, telematics etc.)



Inferred data

Derived from analysis of observation data (e.g. profiling of worker behaviour in the form of risk and fraud assessments.)

These categories of data are often made explicit in guidance documents and privacy policies but not shared with drivers when they download their data or make subject access requests. In our experience, when workers seek out this information, gig platforms aim to make the process difficult and burdensome by engaging in a variety of non-compliant behaviour. Workers seeking comprehensive data have to navigate exceedingly complex and obstructive website architectures and need to circumvent further frustration efforts by support agents, who unnecessarily prolong simple administrative processes or provide automated responses that fail to adequately answer queries.

These procedures can be described as 'dark patterns' designed to guide workers away from exercising their rights as data subjects. On the occasions where workers are able to obtain their data, it is often either missing considerable segments or presented in inconsistent and non-machine readable formats, making analysis effectively impossible. These acts of obstruction force workers to make repeated requests which companies ultimately use as a reason for discrediting them.

In all of the DSAR returns we have seen, no employer has given a full and proper account of automated personal data processing. This is particularly important in areas that can determine security of employment such as work allocation, performance management, safety and security, as discussed through this report. Uber and Ola have argued in court that the safety and security of their platform may be compromised if the logic of such data processing is disclosed to their workers. In our view, safety and security can only be enhanced when platforms transparently set rules and performance standards rather than relying on covert surveillance and summary dismissals, which are some of the key motivators of DSARs.

Given this resistant attitude to DSARs, it is also important to note that many drivers fear retaliation by companies for making requests. When gig platforms perform immoderate and prolonged identity checks in response to subject access requests, workers are easily discouraged and intimidated (see emails sent to drivers by Uber in the platform response case studies). Across the numerous interviews we have conducted with drivers, lengthy confirmation seeking messages, conveyed in complex legal language, have frequently been referenced as deterrents to pursuing requests. For many drivers, the act of persisting with the request is equivalent to putting one's head above the parapet and risking one's livelihood and job security.

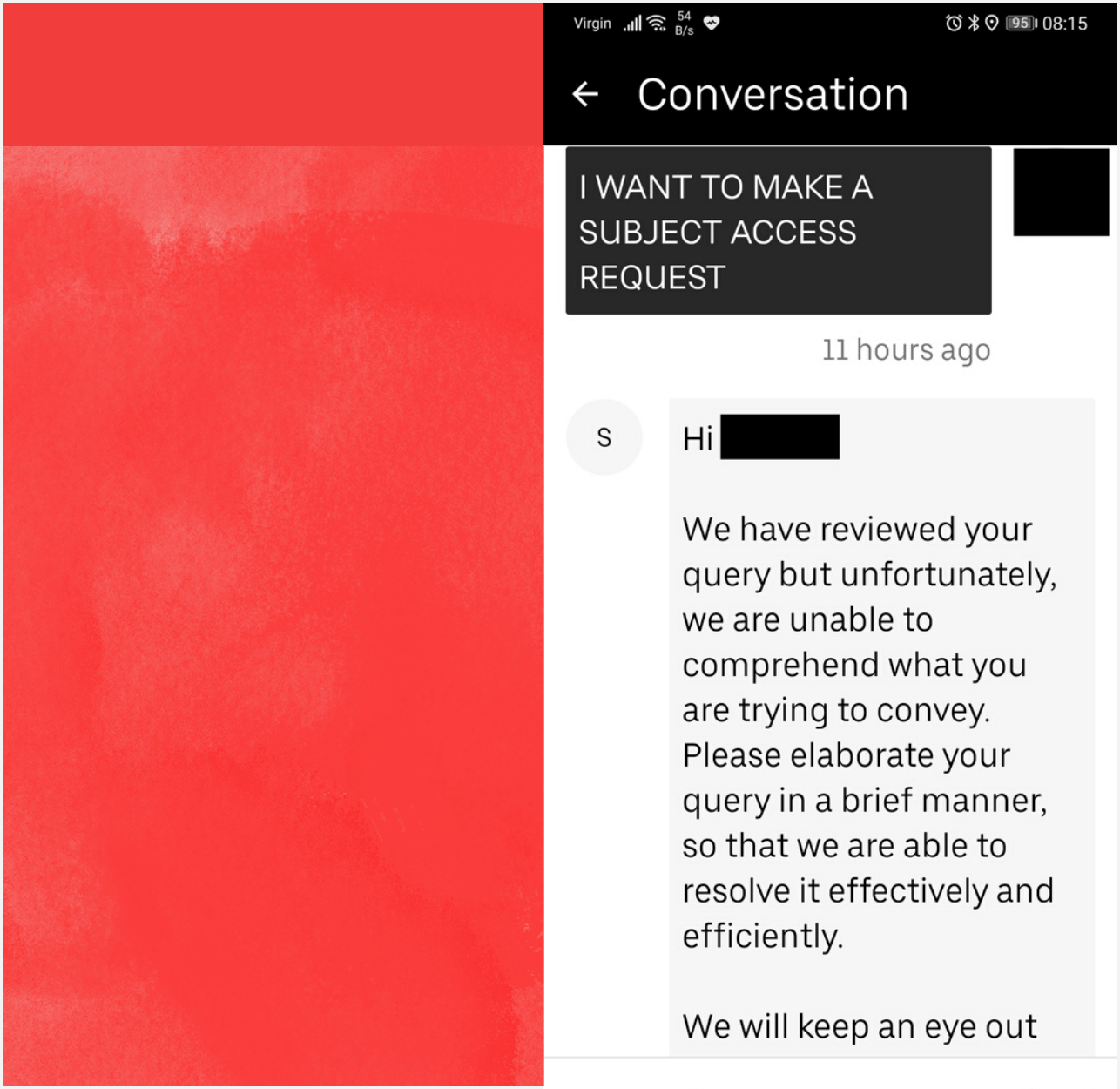
This perception often accrues from experiences of continuous exploitation and insecurity, following from workers' limited ability and knowledge in exercising democratic rights, whether in the UK as immigrants or in their home countries, which in many cases display authoritarian leanings. In a workforce that is already fragmented and prone to economic precarity, where the need for security greatly outweighs the desire to challenge injustice, the impact of this kind of hostile behaviour from companies cannot be overstated.

This insecurity is additionally compounded by the opaqueness of the management algorithms. In the absence of clear explanations of how black-box work allocation or performance management systems work, it becomes very easy for workers to engage in speculative or even conspiratorial thinking on how their interactions with the platform affect their work. This can then extend into a generalised distrust of other institutions and aversion towards organising activity. These are strong and persistent vulnerabilities across the workforce that require particular attention and safeguarding.

Case Studies

Individual DSARs

The following case studies demonstrate some of the ways that Uber engages in obstructive and non-compliant behaviour in responding to data requests by workers. Significantly, these examples cannot be explained away as exceptions or isolated events concerning inexperienced support agents. These responses represent the standard procedures followed by Uber when workers wish to exercise their data access rights.



Case Study

Circular and Futile Answers

M. Ahmed is a former Uber driver and Uber Eats courier. In October 2020, both his Uber driver and courier accounts were suspended, and in February 2021, his driver account was deactivated. This affected his Uber Eats courier account as well, which was subsequently deactivated and deleted.

When Mr Ahmed asked for the cause of his dismissal, he was given contradictory answers. Uber initially cited failed facial recognition checks, and later claimed that the deactivation was due to a high volume of undelivered orders. Throughout the correspondence, they addressed him by the wrong name and ultimately accepted that the messages regarding the failed Real Time ID checks were sent in error. The confusion around his dismissal led him to seek his personal data.

Over the past few months Mr Ahmed has been trying to retrieve the data associated with his deactivated Uber Eats account. Mr Ahmed first tried to obtain his data on 15 April 2021, through the 'Submit a Privacy Inquiry without an Uber Account' form on the Uber website, since his account had been deleted following his dismissal. In response, he received an email from Uber stating:

> "Our Privacy Notice limits our ability to share account holder information. We can only provide this information through the process outlined in our data request guidelines."

This process refers to signing into the account and making the request from within the account.

> "That said, we're able to work with you through the appropriate channels to help as needed."

Mr Ahmed wrote back asking for advice on how he could access the data associated with his now deleted account. He explained that he was writing from the email associated with his Uber Eats account and that he had provided the mobile number associated with this account as well. He added that he was happy to provide further information to confirm his identity.

To this, Mr Ahmed received a response stating that his

> "concern is not related to this account. Kindly write to us from the concerned account or sign-in through help.uber.com with relevant credentials and let us know about the issue so that we can assist you further."

Mr Ahmed wrote back, attaching an image of the onboarding email sent to him by Uber on 03 July 2020, to demonstrate that he was writing from the relevant account. On 19 April 2021, he received the same message stating that his

> "concern is not related to this account."

Mr Ahmed wrote back explaining once again that he is unable to access his account and that he had provided the details associated with his Uber Eats account. He asked to receive guidance on what other information he could provide to identify himself. He received no response.

At this point Mr Ahmed sought help from the App Drivers and Couriers Union and Worker Info Exchange and we escalated the issue with Uber. On 11 May 2021, Mr Ahmed received an email from Uber asking him to confirm the request made on his behalf by us. He wrote back confirming that he had given us his mandate and that he would like his request to be processed.

On 14 May 2021, Mr Ahmed was sent an ID verification form by Uber to process the request. The form asked for the same details he had already shared in his previous messages such as email, phone number, country of residence, the type of data requested. It also asked for his "current rating" – which was inapplicable, as he no longer had access to his account. Mr Ahmed sent the form to Uber, but he did not receive any response.

On 20 May 2021, Mr Ahmed wrote to Uber to get confirmation that they were processing his request. He received no response.

At the time of writing, Mr Ahmed has not received his data. Nor has he been given any explanation of why his request is not being processed.

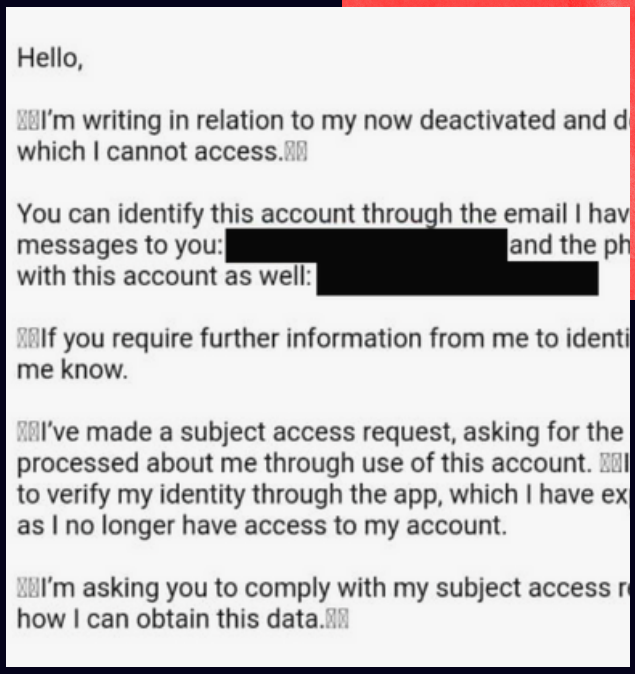
mit a privacy inquiry without an
r account Inbox

Uber Support 17 Apr
/// Please enter your reply above this line. Replies below this line will not be received. \\\\\\ | Support NO

[redacted] 17 Apr
to Uber

please advise on how I can access the data for my now deleted
? I no longer have access to my account however I am writing to y
e email associated with the account in question. I have supplied th
umber associated with the account as well. I'm happy to provide
nformation to confirm I was the account holder. Please advise on
ed. Thank you, looking forward to your response.

oted text



Hello,

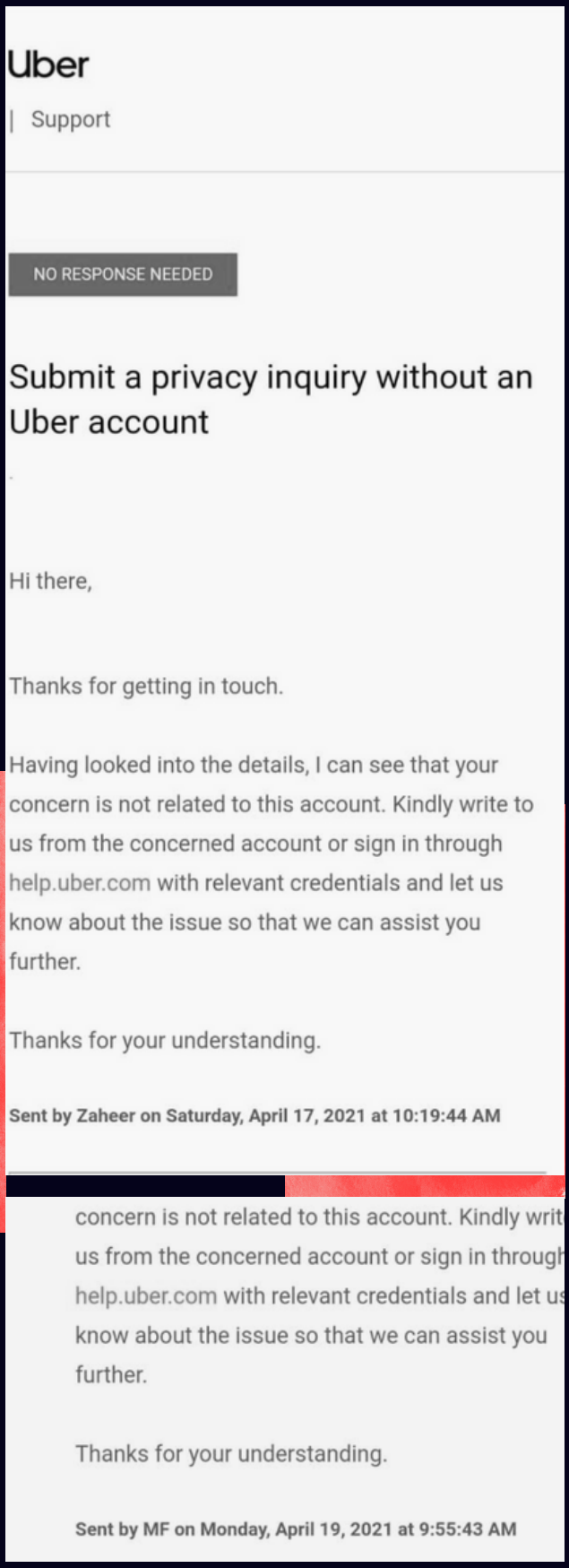
I'm writing in relation to my now deactivated and d
which I cannot access.

You can identify this account through the email I hav
messages to you: [redacted] and the ph
with this account as well: [redacted]

If you require further information from me to identi
me know.

I've made a subject access request, asking for the
processed about me through use of this account.
to verify my identity through the app, which I have ex
as I no longer have access to my account.

I'm asking you to comply with my subject access r
how I can obtain this data.



Uber

| Support

NO RESPONSE NEEDED

Submit a privacy inquiry without an Uber account

Hi there,

Thanks for getting in touch.

Having looked into the details, I can see that your concern is not related to this account. Kindly write to us from the concerned account or sign in through help.uber.com with relevant credentials and let us know about the issue so that we can assist you further.

Thanks for your understanding.

Sent by Zaheer on Saturday, April 17, 2021 at 10:19:44 AM

concern is not related to this account. Kindly writ
us from the concerned account or sign in through
help.uber.com with relevant credentials and let us
know about the issue so that we can assist you
further.

Thanks for your understanding.

Sent by MF on Monday, April 19, 2021 at 9:55:43 AM

Case Study

Inconsistent and Incremental Data Sharing

Mr Amini is a former Uber driver who was deactivated in November 2020 following a failed geolocation check. Uber reported his dismissal to TfL, who then revoked Mr Amini's private hire license, leaving him without work. In a bid to understand the cause of his dismissal, Mr Amini sought to obtain his data from Uber.

Mr Amini made his first request on 13 April 2021 and asked for all of his personal data, including the 26 data categories outlined in the guidance document produced by Uber, as well as the images submitted by him in response to Real Time ID checks. He specified that he wanted data covering the entire period he has been active as an Uber driver.

Mr Amini received a response to his request on 05 May 2021, however the data given only covered the 30 days prior to his request. Since Mr Amini had not been able to work for Uber during this period, many of the datasets provided were blank.

Mr Amini then made another request on 06 May 2021, stating once again that he was requesting data concerning the whole timeframe he has worked with Uber, adding specifically that he wished for data collected through November 2020.

Mr Amini received a response on 28 May 2021. However, he was once again sent incomplete data. Specifically, the Driver Detailed Device Data csv provided by Uber was completely blank.

Mr Amini made another request on 02 June 2021 asking for the missing data. He received his Driver Detailed Device Data for November 2020 on 10 June 2021. However, despite specifying that he wanted all of the data fields listed in the guidance notes produced by Uber, he was sent a restricted data set that omitted 32 of the 50 data fields.

Case Study

Obfuscation and Resistance

Mr Majid is a former Uber driver who was deactivated in September 2020 following a failed geolocation check. As in Mr Amini's case, Uber reported Mr Majid's dismissal to TfL, which caused his private hire license to be revoked. In an effort to understand the basis of Uber's allegations, he tried to obtain his data.

Mr Majid first contacted Uber to request his data on 2 June 2021. In response, he received a message asking him to elaborate his concern in a brief manner. Mr Majid replied with his request for 3 data categories (out of the 26 categories listed in Uber's guidance notes) for September 2020.

On 8 June 2021, Mr Majid got a message from Uber stating:

> "Our Privacy Policy does not allow us to make changes or discuss personal information without contact via the email address associated with your partner account. In order to help you with your specific issue, you'll need to write in using the email address associated with that account. Thanks for understanding."

At this stage Mr Majid contacted us, confused, as he had written to Uber from his account. He wrote back, explaining to Uber that he contacted them by signing into his driver account, so he was definitely writing from the correct email address. He asked if he could provide any additional identification/documentation to assure Uber that he was the one making the request. In response, he got the same message from Uber:

> "Hi...thank you for your message. We understand that you'd like to discuss information related to an Uber account. If you are the account holder, please write in from the email address associated with your Partner-Driver account, and we'll be able to help you right away.

On 09 June 2021, Mr Majid logged into his partner account and started a chat with Uber support to try again. His message asking whether he could make a subject access request was ignored.

On 14 June 2021, Mr Majid contacted Uber once more, stating that he had a query about his driver partner account. He received a response from Uber:

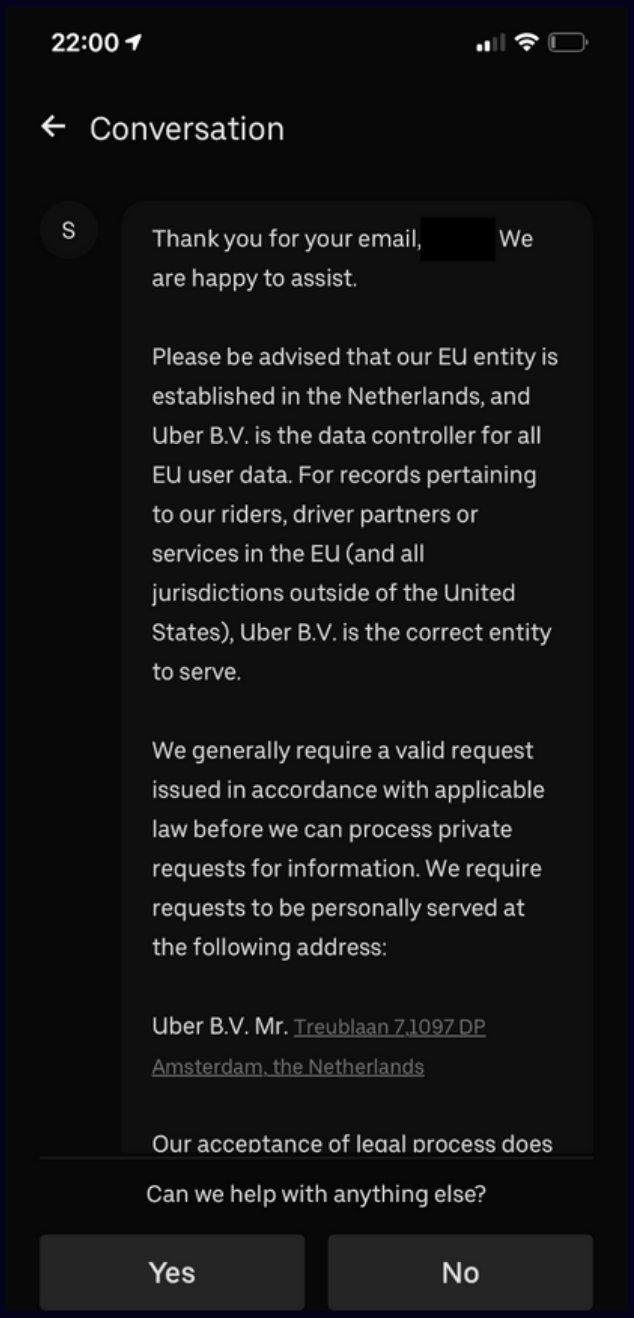
> "Thanks for reaching out…We have taken the opportunity to review your concern and can see that you have previously reached out to us about this issue. One of our team members is currently investigating your issue and we will get back to you as soon as possible. To streamline our communication and avoid any confusion we are going ahead to close out this contact."

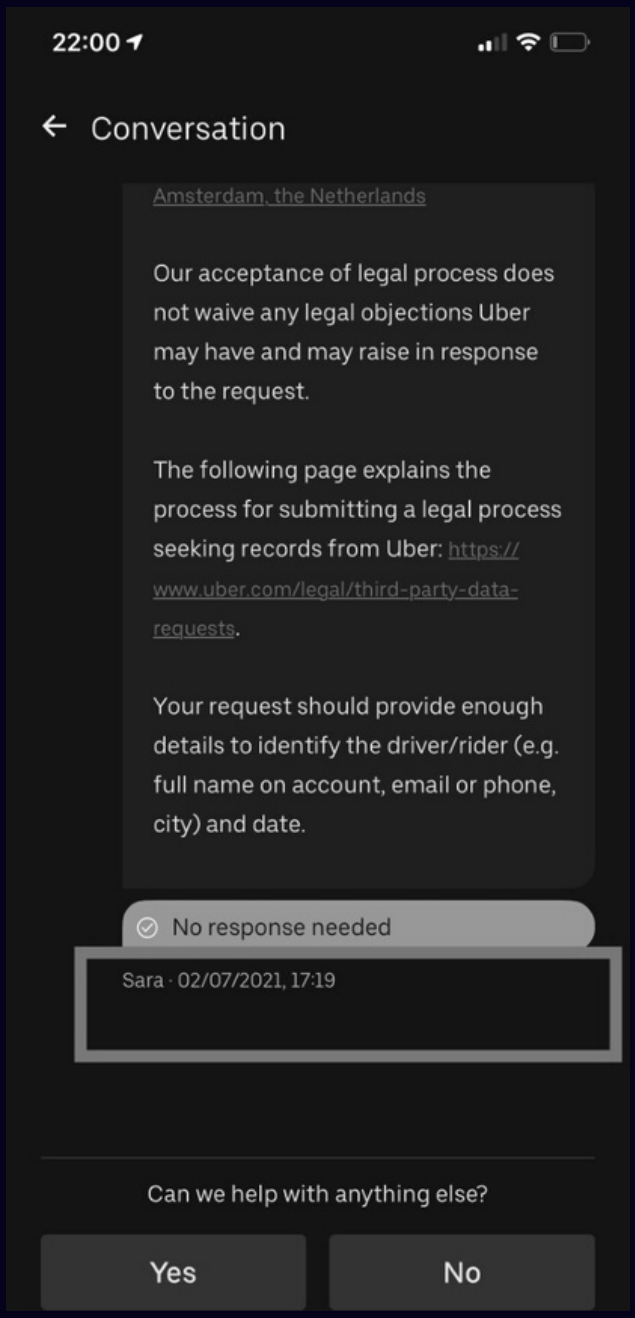
On 16 June 2021, Mr Majid contacted Uber once again, stating that he had been asked to sign-in to his account to make a request, and having done so, he wanted to share details of his request. He received a response the following day, and subsequently sent details of the request (of the three datasets listed above) on 18 June 2021.

Upon receiving no response, Mr Majid contacted Uber again on 28 June 2021, seeking confirmation that his request was being processed. On 01 July 2021, he received a reply stating that his concern had been raised with the specialised team and that they would be in touch to investigate further.

On 02 July 2021, Mr Majid received a response to the message thread he had initiated on 09 June 2021. This message stated that Uber requires requests to be personally served to Uber B.V.'s postal address in the Netherlands.

Mr Majid has not received any further communication.


22:00
Conversation
S
Thank you for your email, [redacted] We are happy to assist.
Please be advised that our EU entity is established in the Netherlands, and Uber B.V. is the data controller for all EU user data. For records pertaining to our riders, driver partners or services in the EU (and all jurisdictions outside of the United States), Uber B.V. is the correct entity to serve.
We generally require a valid request issued in accordance with applicable law before we can process private requests for information. We require requests to be personally served at the following address:
Uber B.V. Mr. Treublaan 7,1097 DP Amsterdam, the Netherlands
Our acceptance of legal process does
Can we help with anything else?
Yes
No


22:00
Conversation
Amsterdam, the Netherlands
Our acceptance of legal process does not waive any legal objections Uber may have and may raise in response to the request.
The following page explains the process for submitting a legal process seeking records from Uber: https://www.uber.com/legal/third-party-data-requests.
Your request should provide enough details to identify the driver/rider (e.g. full name on account, email or phone, city) and date.
No response needed
Sara · 02/07/2021, 17:19
Can we help with anything else?
Yes
No

"The question of algorithms is central to the theme of uberization.

Too often, it is the algorithm that plays the real role of the boss, as technology provides new means for the subordination of workers. There is obviously a need for transparency of algorithmic management but beyond this transparency, there is a need for co-management of the algorithm. Workers' representatives must be able to participate in their development."

Leïla Chaibi, MEP

Case Studies

Platform Responses to Batch Requests by Worker Info Exchange

As demonstrated by the above examples, the individual request processes can be extremely time consuming and capacity intensive. We have therefore created processes to allow us to make batch requests on behalf of drivers and streamline this complex procedure. We have set up a system using the electronic signature and ID solution developed by Scrive to receive a legal mandate from workers to make requests on their behalf. This solution also includes an ID verification run by Onfido (the same ID verification service used by Uber), to ensure that both we and the data controller can be certain of the identity of the requester and preserve their data privacy.

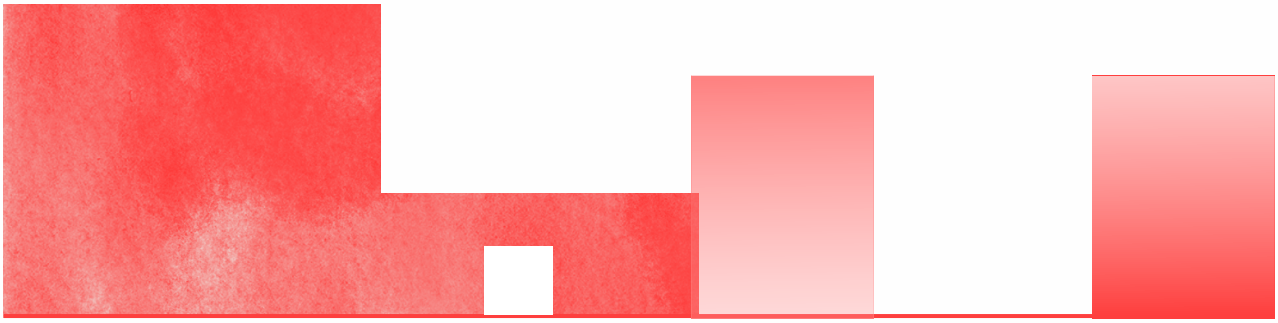
The ID verification requires the workers to submit one of the following ID documents: Passport, Driver's License, Identity Card or Residence Permit. Through this process, an individual consent document is created for each individual that is electronically sealed and verifiable through concealed attachments containing an evidence log to prove the authenticity of the identification process. (Scrive also provides a service to verify the integrity of the consent forms, which is linked to in the documents.) We send these documents, along with a spreadsheet containing the names, emails, addresses and phone numbers of the workers making requests.

Some companies have been amenable and cooperative in responding to requests made through this procedure, while others have engaged in far more obstructive and hostile behaviour. However, even when companies have complied with the requests, there have been consistent issues in establishing the precise data categories collected, as well as obtaining all of the data requested in a structured and machine-readable format. Few companies have been able to provide guidance documents with clear descriptions of the data categories, and the data we've received has often displayed significant incongruities with the processing described in privacy policies.

Generally speaking, companies have shown a tendency to deny the data practices they do not wish to disclose. In one instance, a company claimed that the fraud assessment referenced in their privacy policy had only been undertaken as part of a trial, and that the privacy policy was outdated. Another referred us to a document which they claimed had superseded the one we were basing our request on, even though both documents were updated on the same date.

Despite these difficulties, the most controversial pushback we have faced has been the denial of our right to act on behalf of the workers when making subject access requests as a third party. This unambiguous right (clearly stated in the ICO's guidance and even promoted by the government's GDPR reform proposal) was called into question by both Bolt and Uber.

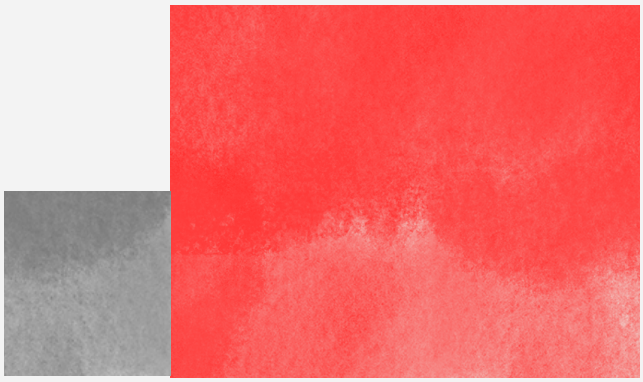
While it is apparent that the resistance acts towards frustrating the request process, it also points to an important gap in the existing guidance on identity verification processes. When companies insist on conducting identity checks by making direct contact with workers, subjecting them to legally complex correspondence, this largely negates the purpose of appealing to third parties for requests. There is a concerning conflict between the rights of the respective parties here that requires urgent regulatory guidance to ensure it is not abused and manipulated to deepen informational asymmetries.



Deliveroo

Out of the seven companies we have made requests to, Deliveroo was the most compliant. In our requests, we asked companies to confirm the date by which the request will be answered and to process the requests in bulk, informing us when all individual disclosures are made.

Deliveroo responded to the requests within the legal time limit, provided a guidance document, clearly annotating the data categories and communicated with us through the process.



Amazon Flex

Amazon Flex initially responded to the requests by asking for identification of the data subjects, however, upon receiving an explanation of the verification carried out through Onfido, they agreed that sufficient information had been provided about the data subjects to fulfil the requests.

Following the confirmation, Amazon Flex informed us that they would require two additional months to respond fully to the requests.

Amazon fulfilled the requests within the stated time frame however initially failed to produce a guidance document offering an explanation of the data categories or data fields, which rendered much of the information unintelligible as it was not clear what the units or metrics of measurement were for many of them. They also sent all of the data in pdf format despite our specification for a machine readable format such as a csv.

We subsequently wrote to Amazon to address these omissions and were able to obtain both a guidance document and the data in a machine readable format.

Just Eat

Following the confirmation of the requests, Just Eat informed us that they would require two additional months to respond fully to the requests, and that they would provide the data by September 2021. Just Eat provided the data by the specified date and communicated that they had processed the DSARs, as we had requested.

The data included extensive location information (in pdf format) but did not provide any of the other categories we had requested, such as metrics for assessing compliance with operations and/or successful delivery. A guidance document was not provided.

When we shared our findings with Just Eat, they strongly contested that they had failed to provide the data requested. Just Eat argued that they had provided us with courier onboarding and communications data, as well as route and location data. Most of the requested data, Just Eat maintained, was either not processed; or deleted in line with data retention policies; or contained technical or confidential information about the conduct of their services; or included personal information of third parties.

In response to our request for a guidance document, we were referred to the privacy policy.

Ola

Ola confirmed receipt of the requests a month after they were filed and the drivers received responses a month after Ola's confirmation. The data consisted of a spreadsheet containing only the information input by the driver when signing up, such as name, phone number, national insurance number, payment details; along with the average rating.

We subsequently wrote to Ola to express our concern that the data given did not cover many of the categories listed in Ola's 'How we process your data' page. Ola responded by referring us to the privacy policy, suggesting that all other information was outdated and superseded by the privacy policy.

We explained that the dates on the two documents indicated they had been updated at the same time. The categories we referred to appeared to be a detailed breakdown of the data processing described in the privacy policy. We did not receive further communication from Ola.

Free Now

Free Now complied with our request within the expected timeframe and has been responsive through the process however, we encountered a few issues worth highlighting.

Free Now initially attempted to direct us to their online contact form to make the request. This did not support the size of the documents we needed to share. We were only able to obtain the DPO's email after repeated emails explaining the issue.

The data we received did not cover some of the data categories we had asked for, such as data relating to the "random forest" algorithm used for fraud prevention. This is explained in the driver privacy policy which states: "Based on the calculated score we are able to prioritise the dispatched journeys accordingly. This ensures a fair and risk minimised dispatchment." When we pointed this out, Free Now stated:

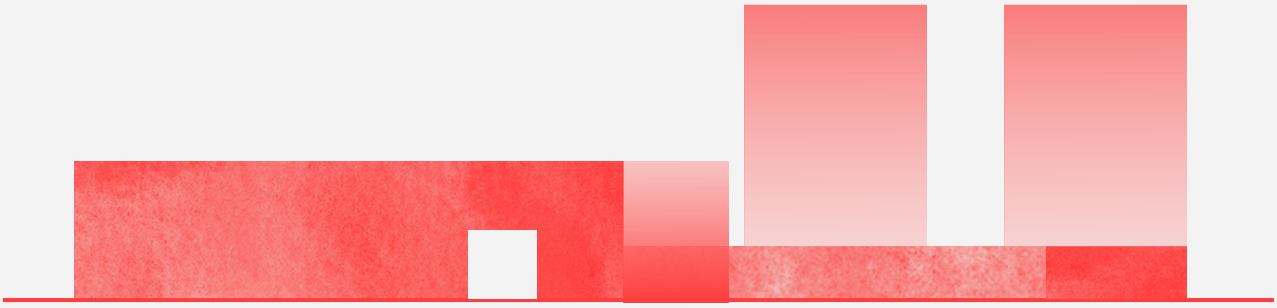
> "We do not process fraud scores on our drivers, and we do not use (and have not used) the fraud-detection algorithm in relation to our drivers and/or their personal data. Section 3.4 of our driver privacy notice therefore requires updating in this regard and we regret any confusion about this. By way of background, we first introduced this section into the notice in relation to testing that was being carried out by our Revenue Assurance Department. However, no drivers were ever included in this testing, and therefore no driver-related fraud scores (or similar) have been created. We have since stopped carrying out this testing."

In response to our request for an accompanying guidance document offering descriptions of the data categories, we were advised:

> "Given the accessible, concise and intelligible format of the data in question, no additional guidance is required in respect of these requests."

Free Now updated its privacy policy in September 2021, following our correspondence in June 2021. However, the section regarding the fraud detection algorithm remained. We approached Free Now for comment on this discrepancy prior to the publication of the report in November. Free Now then informed us that the privacy policy was updated on 30 November to reflect the absence of the random forest algorithm. Free Now's new privacy policy now states the following:

> "In order to prevent fraudulent activity, we store your GPS location data sent to us by your mobile device at short intervals from the time of acceptance until the end of a tour. This allows FREE NOW to create a map of the entire course of a tour. In this way, we want to ensure that drivers do not deliberately extend the route in order to achieve a higher fee. At the same time, we can rectify unjustified passenger complaints by being able to follow the actual course and route to a tour. The processing of your GPS location data during a tour takes place for your own protection, as well as for the protection of the passenger and for our protection on the basis of Art. 6 (1) f) GDPR."



Bolt

Bolt ignored our request made on 27 April 2021. We were only able to get a response after making a complaint to the Estonian Data Protection Inspectorate, Andmekaitse Inspektsioon (AKI), Bolt's lead supervisory authority. On 24 May 2021, AKI instructed Bolt to respond to our request by 04 June 2021. On 04 June 2021, we received an email in which Bolt claimed not to be in receipt of the documents we had sent them:

> "We have received through our lead EU supervisory authority, namely, AKI, your correspondence addressed to Bolt, "via email", dated 27 April, 2021.
>
> AKI wrote to us on 24 May asking Bolt to respond to your correspondence. Wae are in receipt of your letter only, and none of the attachments referenced within your correspondence.
>
> Your request, dated 27 April 2021, seeks the porting of personal data of data subjects - i.e. drivers - said to be under your mandate.
>
> Identity verification
>
> Bolt is not in receipt of the name of any data subject said to be under your mandate.
>
> The Worker Info Exchange is said to, in your correspondence, have identified and authenticated each driver. While this is appreciated, it is for the controller, Bolt, to use all reasonable measures to verify the identity of a data subject who has made a request for access to their personal data. Bearing in mind that we are only in receipt of your letter, dated 27 April 2021, communicated through AKI, we have no means of inspecting nor satisfying ourselves of the verification, and ensuring that appropriate technical safeguards ensure the authenticity of these requests.

> Supervisory authority jurisdiction
>
> Bolt is committed to upholding user rights, affords a complaints channel, and engages with AKI and other supervisory authorities enthusiastically wherever necessary. In this instance, however, we are not satisfied that the Worker Info Exchange is competent within the meaning of the GDPR to lodge a complaint with AKI on behalf of data subjects."

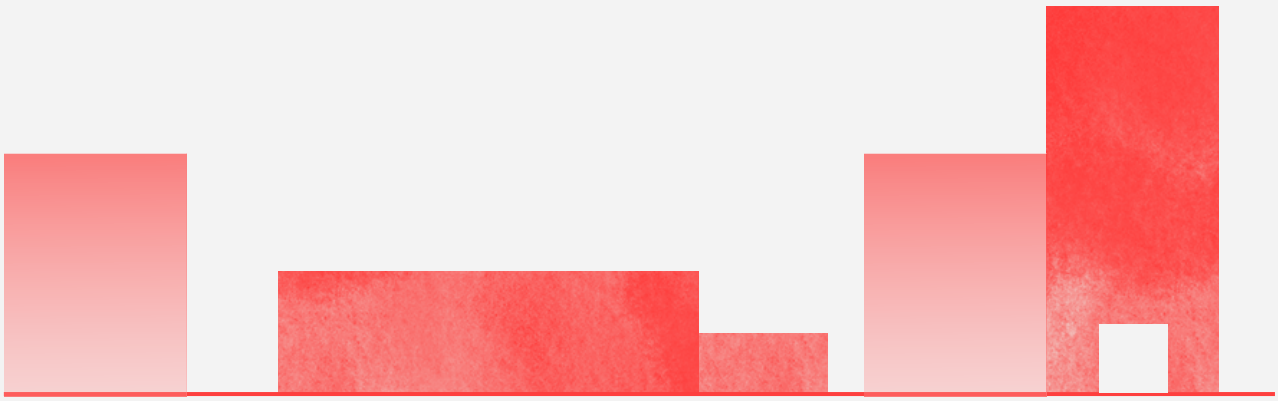
We replied immediately, appending the mandate documents we had sent to Bolt on 27 April. Bolt did not reply. We sent a follow up email to confirm Bolt's receipt of the documents on 16 June 2021, this too was ignored.

Finally, in October 2021, after further escalating the matter with AKI, we received an acknowledgment of our data requests from Bolt. In the correspondence, Bolt once again challenged our ID authentication process while claiming that many of the data categories we had requested fell outside the scope of data portability.

It is unclear to us why some of these categories (such as 'efficiency ratings' as specified in the privacy policy) did not fall within the scope of the subject access requests. Access is provided, we were told, to drivers regarding trip data and that sharing any further route information would infringe on the rights of others and be "commercially devastating" for Bolt:

> Therefore, in principle, Bolt would have looked to comply - having satisfying the relevant authentication checks - with any such portability request through the provision of that which remains within the scope of the obligation:
>
> - Name, e-mail, phone number, place of residence.
> - Information about vehicles (including registration number)
> - Driver's license, photo, profession and identity documents.
>
> This information is already available to Bolt Drivers in the account portal, and can be inspected and retrieved."

Additionally, we assisted a Bolt driver who had been trying to obtain his data, to make an individual request to Bolt. Bolt had been ignoring repeated requests by the driver since August 2020. The driver made a complaint to AKI and Bolt was instructed to respond to his request by 16 June 2021. The driver was eventually sent some data, (mostly data provided by the driver himself, such as the documents he submitted during sign-up) however this did not cover a number of important data categories such as location data, route information or efficiency ratings. The driver was not offered an explanation of why he was not given these datasets.



Uber

While processing the requests, Uber chose to take issue with the process we set up for making requests on behalf of drivers. Uber tried to invalidate the requests we made on 20 April 2021 with the following response:

> "Thank you for your emails. Based on the information provided to us, we can only conclude that Onfido might be able to verify whether an individual is who they say they are, but not whether the details they provided correspond to those of their own driver account on the Uber app. The process also does not provide us with evidence that the relevant drivers actually asked the ADCU or WIE to represent them in the exercise of their data subject rights.
>
> Aside from whether or not the ADCU or WIE, or any representative body, under GDPR can represent data subjects in the exercise of their rights, we have received multiple responses from drivers indicating that they never authorised the ADCU or WIE to make such a request on their behalf. In a few cases this request was called "a scam". So we cannot conclude without reasonable doubt that the individuals on whose behalf you are making a request, are actually the account holders of the relevant driver accounts. And even though the process may verify the identity of a data subject, we cannot verify whether it is the correct data subject. As per ICO guidance and art 12 (6) of the GDPR, our processes are designed to verify the identity of the account holder before we disclose any personal data."

With this response, Uber opted to verify the requests by sending the following email to the drivers: (Uber's message mistakenly refers to ADCU rather than WIE, as a similar request was made by ADCU on 2 March 2021.)

> "Uber has recently received a portability request related to your email address through the App Drivers & Couriers Union ("ADCU").
>
> Uber has implemented the appropriate measures to respond to the exercise of data subject rights in line with the EU General Data Protection Regulation ("GDPR"). The first step in responding to these is to without reasonable doubt verify the identity of the requester, in order to ensure that it is in fact the account holder making a request, and to ensure the protection of personal data, in particular against unauthorized access.
>
> The received request does not enable Uber to verify the authorization given by the data subject for an access request made by a third party, nor to verify without reasonable doubt the identify the requester as the account holder. We also reiterate that for the exercise of the rights of access or portability, Uber's policy is to always require identification identical to the identification used for its services. The identification is based on the on-line identifiers collected and verified at the time of signup of the account or subsequently changed and re-verified: the email address, the telephone number, the password and when applicable a verification pin sent via SMS.
>
> Therefore, Uber is not able to comply with the request received through ADCU. In order for us to process the portability request, and in line with ICO guidance, we decided to write to you directly and kindly ask you to confirm the request by responding to this message through in-app support."

Uber finally began processing the data portability requests towards the end of June, over three months after the original request had been submitted. In these portability requests, Uber only shared six categories of data, containing information or documents submitted by the drivers themselves, citing the recent transparency case (see Uber's response below for link) we brought against Uber. Uber claimed that the court had confirmed the rationale for data portability as preventing lock-in, which they took as a pretext for sharing limited data:

> "With reference to your data portability request, we herewith provide you with your data and an explanation of what data categories are provided.
>
> Due to recent legal developments and case law relating to Uber (http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2021:1020),
> we have assessed our processes for responding to data portability requests to make sure we comply with all applicable requirements when responding to such requests. In this regard, we have taken into account that the rationale for data portability is to prevent a 'lock-in' of the data subject, as was recently confirmed by the court.
>
> Following this assessment, Uber will provide personal data that has been knowingly and actively submitted by you to Uber and which does not adversely affect the rights and freedoms of riders as part of the response to your portability request.
>
> We will therefore be providing you with the following data categories:
> Driver Account Profile Info
> Rider Account Profile Info
> Driver documents
> Driver Trusted contacts
> Driver Profile information
> Rider/Eater/Driver Saved locations
>
> In case no data has been provided for one of the above categories, that file for that category will remain empty."

Uber then began returning the subject access requests in September, nearly five months after the requests were filed. In these responses, we finally received most of the data categories we asked for, and explanations for why we didn't receive others.

Data Requested & Received

Driver and rider account profile information
Driver online/offline
Driver lifetime trip data
Driver app restrictions
Rider lifetime trip data
Driver star power requests
Driver and rider device data
Ratings
Real Time ID pictures
Driver communications data
Safety Complaints
Driver performance badges
Driver trip status
Account Bliss tickets
Driver cancellations from riders
Driver dispatches offered and accepted
Payment methods

Data Requested & Partially Received

Driver detailed device data
Driver and rider communications data
Rider detailed device data

"To be able to expedite your request, we have limited the timeframe of the categories 'detailed device data' and 'driver and rider communications' to the last 30 days. If you are looking to receive more data of these categories we ask you to specify your request due to the fact that large quantities of data have to be retrieved manually for these data categories."

Data Requested & Not Received

Driver GPS data
Rider GPS data

"GPS data is not included, due to the impact the provision of a large amount of GPS data can have on the rights and freedoms of others, as it would give insights into the movements and travel behaviour of passengers. If you are looking to receive GPS data, we ask you to specify your request to a specific, limited time frame, so we can assess your request accordingly."

Invoices
Account call recordings
Account Zendesk tickets

"With regards to Zendesk tickets, call recordings and invoices, we ask you to specify your request to a specific, limited time frame, due to the fact that large quantities of data have to be retrieved manually and/or reviewed for personal data of others for these data categories."

Driver documents

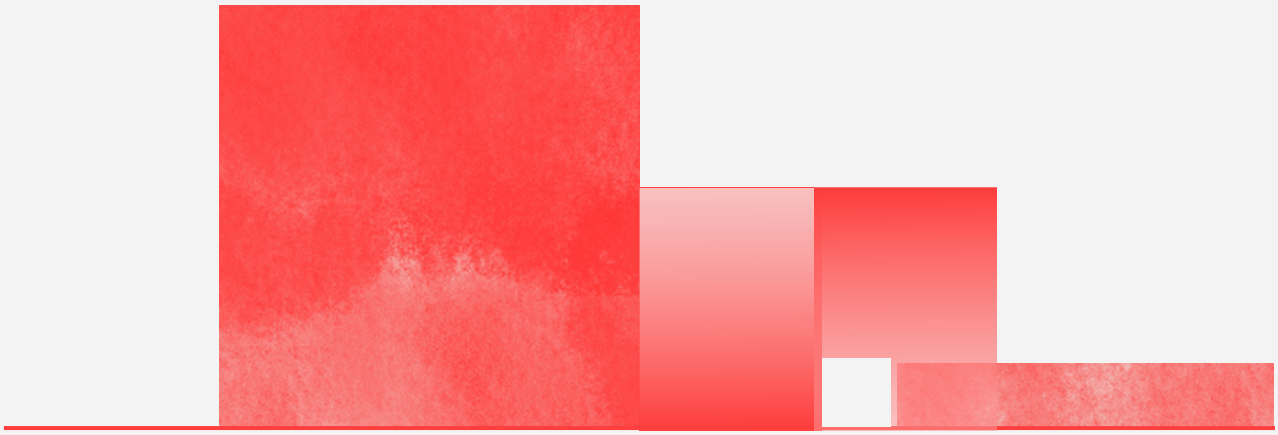
"Your driver documents were already provided as part of the recent response to your data portability request and are therefore not included in this response."

Telematics

"Please note that we do not store telematics data anymore other than the data that is provided in the detailed device data files."

However, despite our specification for Uber to process the requests in batch and notify us at each stage of the process, Uber has chosen to handle the requests in a piecemeal way, and without clear communication, creating further challenges in tracking the completion of the DSARs.

In 2019, Uber did provide telematics data including braking and acceleration data in data subject access request returns. Indeed, Uber provided drivers with a daily update in the app on the number of incidents of smooth braking and acceleration. Then in 2020 and 2021 Uber stopped the daily in-app notifications and stopped providing this data when drivers made DSARs even though Uber's privacy policy has maintained that such data was being processed. This suggests that either Uber stopped processing critical safety data, to limit the risk of classification as an employer, or Uber processed this data all along but continues to deny drivers the right to inspect and access the data.



Part III

Exercising Data Rights at Work: Strategic Litigation

Overview

The issues listed above illustrate the need for turning to litigation in the exercise of digital labour rights. To this end Worker Info Exchange has assisted several groups of drivers from the UK, the Netherlands and Portugal in bringing three separate cases against Ola and Uber at the Amsterdam District Court, invoking drivers' rights as defined by Articles 15, 20 and 22 of the GDPR. We brought the cases to challenge insufficient data access and transparency in algorithmic decision-making. The data controllers for both firms are based in the Netherlands and so it was possible to bring common action there on behalf of drivers from multiple jurisdictions.

Our goal in bringing these cases was to set and confirm a transparency standard for subject access and data portability disclosures that might be applied consistently at the individual and collective level. Setting such a standard would help create a replicable model that can be applied with different companies across the gig economy as well as in different sectors and industries. This would contribute to a richer and healthier worker data ecosystem enabling algorithmic harms and inequalities to be identified and challenged. With these cases we aimed to establish that the burden of proof rests upon the data controller to disclose in full what data categories it processes, including the observed and inferred data categories (referenced above). We also expected to receive meaningful disclosure about the existence of automated decision making workers are subject to including profiling. We argue that platform workers cannot have full knowledge of or be specific in their requests until the data processor first commits to transparency.

Uber Drivers v. Uber I	On 20 July 2020, a group of drivers brought a case against Uber B.V., which is established in Amsterdam and acts as data controller for all data processing regarding drivers in the European Union. This case challenged the insufficient data shared by the company in response to subject access requests, which were based on Uber's guidance document cited earlier in this report. In this case, some drivers were missing as many as 19 of the 26 data categories listed in the guidance document.
Ola Drivers v. Ola	On 9 September, a similar complaint was filed against Ola Cabs. In this case, the DSARs were based on Ola's data processing document. As in the Uber case, the Ola drivers had been able to obtain a very small portion of the data Ola collects and processes about them.

Uber Drivers v. Uber II

Additionally, on 26 October 2020, four Uber drivers from the UK filed more specific complaints, demanding transparency of automated decision-making, including profiling, as well as the information about the underlying logic involved and the envisaged consequences of such processing for the drivers. In each of the cases the drivers were dismissed after Uber said its systems had detected fraudulent activity on the part of the individuals concerned.

The Court handed down judgments on 11 March 2021. The court admitted all the individual applications, except those of two Uber drivers. In all three cases, the court rejected Uber's argument that drivers taking collective action to seek access to their data amounted to an abuse of data protection rights. The fact that the applicants and the trade union to which they were affiliated might have other interest in obtaining personal data, namely, to use it to obtain clarity about their employment law position or even to gather evidence in legal proceedings against Uber, did not constitute such an abuse. These considerations by the court acknowledge the right of third parties, such as Worker Info Exchange, to exercise data rights on behalf of workers.

Uber Drivers v. Uber (General Transparency Requests)

In this case, the court rejected some of the complaints of the Uber drivers for a number of reasons. Firstly the court held that, in the given circumstances, it was not enough for the applicants to rely on the principle of transparency. Uber was allowed, in accordance with recital 63 of the GDPR, to ask for a specification of the personal data that applicants wish to receive because it processed a large amount of data. The request with regard to a number of data categories (e.g., Driving Behaviour), was therefore denied.

The court held that the internal referrals or reports that were included in the driver's profile maintained by management did not contain any information about the data subject that could be verified by the data subject themselves. In this case the driver profile referred to was a profile apparently maintained by support staff who would update the profile with notes and tags relating to customer and/or driver complaints, comments and queries. Uber was therefore only obliged to provide the data about applicants that form the factual basis of the notes maintained and not the internal notes and tags maintained by management which we say amounts to performance monitoring and management.

The drivers requested information on data processed in Uber's so called 'upfront pricing system' which determines fixed pricing for customers before the start of a journey, based on a predicted route the driver is expected to follow. However, the court noted that the drivers did not substantiate that they wanted to be able to verify the correctness and lawfulness of the data processing. This part of the request was therefore regarded as no more than 'a wish to gain insight' into how Uber uses algorithms to manage trip performance. The court concluded that art. 15 GDPR does not support this goal.

The court also denied the request for information about automated decision-making and profiling relating to work allocation. While it was obvious that the batched matching system and the upfront pricing system did have some impact on the performance of the agreement between Uber and the driver, the court saw no evidence of any legal consequence or significant effect, as referred to in the Guidelines and art. 15 (1) sub h GDPR.

Finally, the court held that Article 20 GDPR did not require Uber to provide certain categories of personal data in a csv file or by means of an API. Except for the data provided in pdf format, Uber had provided the personal data in a format that allowed the applicants to transmit this data to another data controller as required under Article 20.

The court also considered whether certain categories of data had to be transferred in a machine readable format. The data categories in question included 'Zendesk Tickets', 'Driver Complaints' and 'Invoices'. The court ruled that these data categories do not fall within the scope of Article 20 of the GDPR, because the data had not been provided to Uber by the claimants themselves. Therefore the court saw no reason to order Uber to transfer these documents in a format other than the pdf format.

The court decided that drivers' request for personal data transfer in csv format was based on a wish to aggregate the data to improve their collective negotiating position, and that the purpose of data portability is preventing lock-in. While this has not presented us with immediate difficulty, the court's analysis of the limitation of data portability rights for the purposes of setting up a data trust is interesting. In our opinion, the right of labour to bargain is congruent with the Article 20 objective of preventing lock-in.

Ola Drivers v. Ola (General Transparency Requests)

The judgment in the case against Ola Cabs resulted in a few important wins. Ola was ordered to disclose:

> 1) Rating data, in anonymised form, to the extent that this data was not available through the Ola app.
>
> 2) Personal data of the applicants that was used to generate 'fraud probability scores' and 'earnings profiles' that were maintained on every driver.
>
> 3) Personal data of the applicants that was used in Ola's Guardian surveillance system to identify what Ola describes as 'irregular trip activity'.

In the case of one applicant, the court decided that a decision to make deductions from driver earnings amounted to an automated decision lacking human intervention. **We believe this to be the first time that an algorithmic decision was qualified as an automated decision in the sense of art. 22 GDPR by a European court.**

Ola was ordered to provide information on the choices made, data used and assumptions on the basis of which the automated decision was made, in a transparent and verifiable manner. Ola was also ordered to communicate the main assessment criteria and their role in the automated decision, so that drivers can understand the basis of decisions and check the correctness and lawfulness of the data processing.

Uber Drivers v. Uber II (Transparency on Automated Decision Making)

In the case of the group of drivers who filed on July 20, 2020, the court rejected the claim that the decision to terminate the drivers' employment was based solely on automated decision-making according to Article 22 of the GDPR. In the absence of evidence to the contrary, the court accepted Uber's account of its internal procedures and concluded that there was meaningful human intervention in each of these cases.

However, the judgment produced a significant win as well. With regard to two of the applicants, the court found that Uber had not clarified which specific fraudulent actions resulted in their accounts being deactivated. Based on the information provided by Uber, these applicants could not verify which personal data Uber used in the automated decision-making process that led to the decision to terminate their employment. As a result, the decision to deactivate their accounts was insufficiently transparent. Uber was therefore ordered to provide access to the personal data used for the decision to deactivate their accounts, in such a way that applicants would be able to verify the correctness and lawfulness of the data processing.

For the six drivers who filed complaints on October 26, 2020, Uber failed to defend these cases and a default judgment was entered in favour of the drivers on February 24, 2021. Uber was ordered to reinstate the drivers and to pay compensation for lost income as well as damages. Many of the London drivers had their licenses revoked by Transport for London on the back of Uber's allegations of fraudulent activity. We supported all the drivers who appealed the revocation at the City of London Magistrates Court and all of them had the revocation decision overturned. See more on this in the London Appeals section of this report.

Appeals

Currently, the three judgments in the Uber and Ola cases are pending before the Court of Appeals in Amsterdam. In its decisions of 11 March 2020, the Amsterdam District Court ruled that the drivers were admissible. The appeal of Uber and Ola for abuse of rights was rejected. In addition, several requests from the drivers were granted, such as the access request regarding the use of driver surveillance systems and the data used as the basis of the unfair dismissal of two drivers.

Nonetheless, a large part of the access requests were rejected. We believe in several instances, the court applied a too narrow or incorrect interpretation of the transparency principle and of the rights of data subjects. The court also seemed to struggle with the technical and legal complexity of the data processing by Uber.

On appeal, the drivers raise, inter alia, the following objections to the District Court's ruling:

1) The consideration that the drivers should have more closely specified their requests is incorrect;

2) Tags, reports, ratings and GPS-data fall within the scope of the right to access.

3) Uber and Ola cannot refuse access by invoking the 'rights and freedoms' of passengers.

4) The District Court failed to acknowledge that Uber's decisions regarding deactivation of drivers qualified as automated decisions in the sense of art. 22 GDPR, since these decisions affected the drivers considerably and Uber did not show evidence of meaningful human interference.

"Workers can only effectively challenge decisions if they know how or why they were taken. In this context knowledge is power. Transparency and strong rules can empower workers in the digital age. But to end the era of 'computer says no' at work, we need a new and robust set of digital labour rights for the 21st century. Besides transparency we need to stop the arbitrariness, constant surveillance and extreme workload that comes with having an algorithm as a manager. Platforms must no longer be able to hide behind their algorithms and enlarge the power imbalance between employer and employee through technology."

Kim van Sparrentak, MEP

London Licensing Appeal Cases

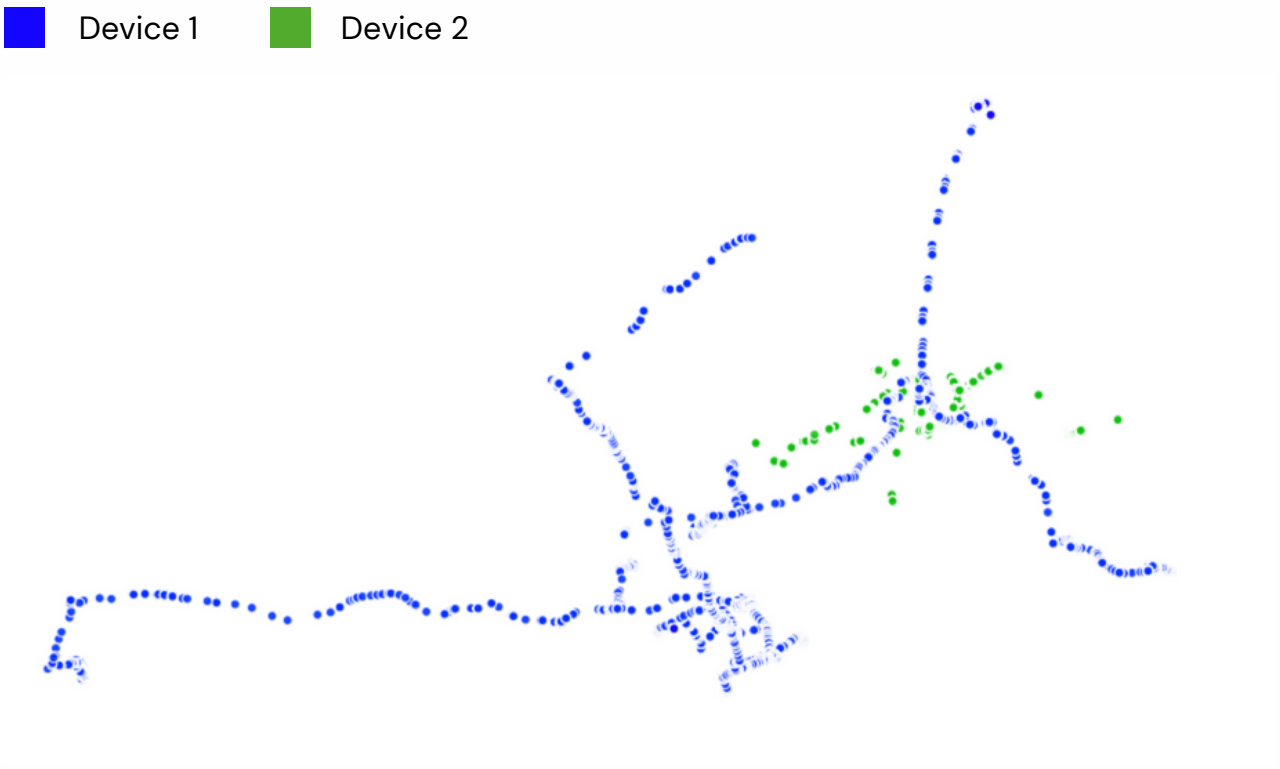
A Flood of Complaints

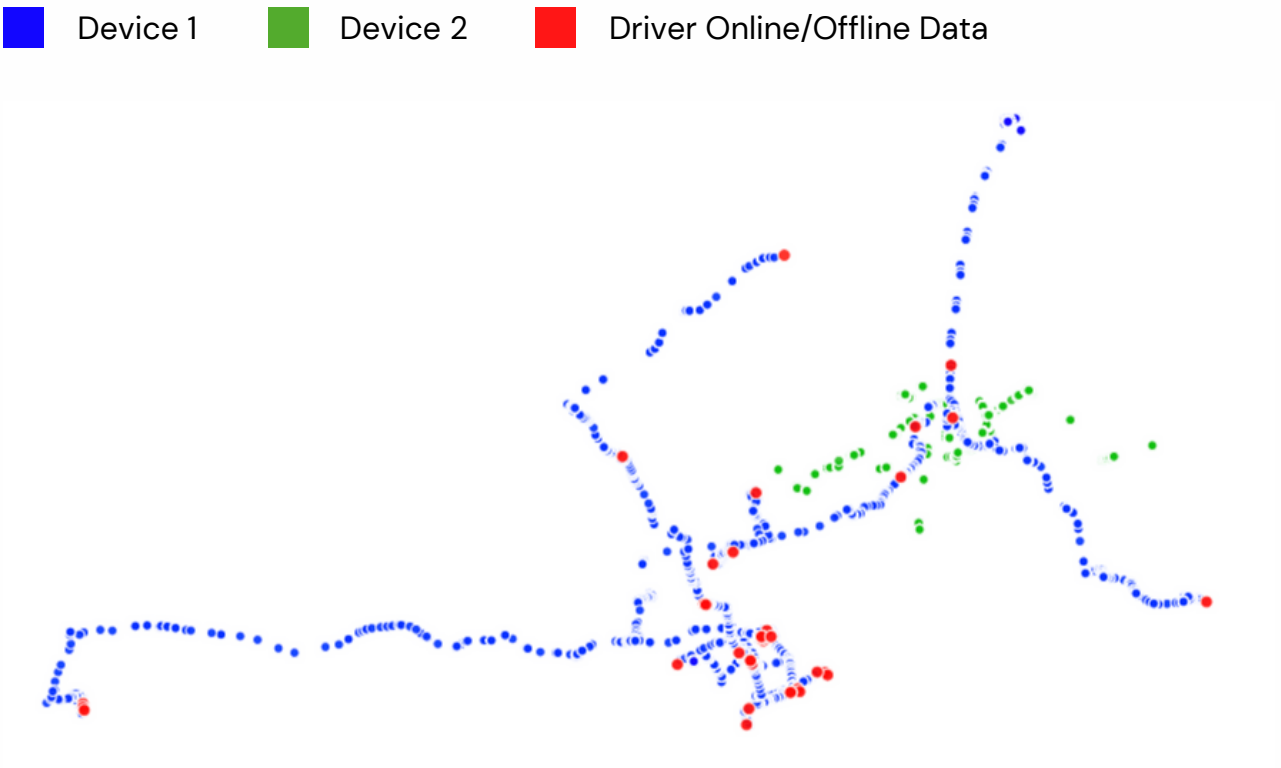
In the past year we have supported more than a dozen drivers as they pursued appeals in the courts against decisions made by Transport for London (TfL) to revoke driver licenses after allegations of app based fraud from operators such as Uber. TfL is responsible for licensing and regulating the taxi and private hire trade in a dual tier market, regulated separately under different legislation. TfL is responsible for assessing the fitness of drivers and operators to be licensed and operators are required to refer all driver dismissals to the regulator for a fitness assessment.

Freedom of information requests have revealed that TfL received 10,169 notifications of driver dismissals from licensed private hire operators in London for the twelve month period ending August 31, 2021. This represents a 123% increase over the same period the previous year. For the period, TfL reported there were a total of 105,000 licensed private hire drivers and 78,000 available licensed private hire vehicles. Given that driver licenses carry a three year term compared to one year for the vehicle license, the latter is normally considered a more reliable indicator of the true number of working drivers available for the period. But for the duration of the pandemic, demand for ride-share services were dramatically reduced with Uber reporting bookings down by 50% on average for the year.

It is likely that the majority of the reports came from Uber as the largest private hire operator in London. This could equate to as much as 20% of the available workforce for the period being dismissed. We suggest given the volumes and lack of a meaningful human involvement in the dismissal decision, many of these decisions were taken and executed by automated and semi automated means.

These dismissals are often due to problems associated with Uber's Real Time ID (RTID) system: facial recognition and geolocation checks (as discussed in Pa Edrissa Manjang's and Aweso Mowlana's cases), which wrongly determine that drivers are engaging in account-sharing, if multiple devices linked with the driver account are found to be 'accessing' it from disparate locations at around the same time. In another case we examined, we were able to retrieve an additional data set called the driver online/offline data, which "provides data on when the driver went online and offline, also referred to as 'driver state." The different states that the driver can be in are Open, En Route, On trip and Offline. We then compared the location data of the two devices with the driver online/offline data. This also revealed that only the device carried by the driver had been used to go online.


Device 1
Device 2


Device 1
Device 2
Driver Online/Offline Data

Regulatory Pressures

These cases point to significant issues with how worker fraud is defined within platform company policies. As we have discussed previously in the report, it is clear that these instances do not refer to acts of criminal fraud but rather failures in meeting opaquely set performance metrics. The successful reversal of these revocation decisions has consequently hinged primarily on Uber's failure to comply with our DSARs and provide any evidence of actual fraud or wrongdoing. This has been highlighted many times in court, where it has been noted that at no stage in these cases has there been a risk to the public, and that TfL has proceeded straight to revocation, without any investigation into actual events.

It is at this level of regulatory enforcement that we see a dire lack of scrutiny, not only perpetuating the automation set in motion by gig platforms, but also encouraging it. There is evidence that the regulator has also been demanding anti-fraud detection and reporting, which operators are pressured to do at the risk of losing their own license. Court documents from Uber's 2020 licensing appeal reveal that TfL reviewed the Data Protection Impact Assessment (DPIA) for the RTID system in March 2020. Our FOI request to TfL to provide us with a copy of the DPIA was refused on grounds of the necessity of TfL maintaining confidentiality with Uber as a regulated entity.

Nevertheless, given that TfL did review the document and the requirement that Uber inform TfL of any infringement of data protection law, TfL must accept culpability for the use of such flawed surveillance as RTID and the devastating impact this has had on the lives of so many wrongly accused drivers.

In 2015, TfL issued a proposal for consultation to:

> "make it a requirement that app based platforms have, and can demonstrate during pre-licensing checks and compliance inspections, appropriate security measures to prevent the app being used by a person other than the licensed driver they are allocating bookings to."

TfL went on to specify the technological solution they expected to see:

> "Our preference is for operators to design a system whereby, whilst available for work for an operator, the driver must periodically log back in to their booking app, for example via facial or fingerprint technology, thus minimising the possibility of the account being passed off for use by another driver."

The independent regulatory integrated impact assessment failed to identify the scale of the problem TfL was seeking to address noting,

> "there is presently an absence of industry-wide data on the level of security currently in place."

Even more concerning is that the impact assessment failed to acknowledge any impact on drivers from the imposition of invasive workplace surveillance tech, though they did recognise the cost impact for operators and minor to moderate benefits for passengers. In the end, no proposal was taken forward but TfL pledged to:

> "explore options to ensure that where operators use app-based platforms, that these are safe and secure and cannot be fraudulently used."

However, despite the absence of a regulatory standard, TfL has fostered the introduction of such standards as a condition of licensing for Uber, Free Now and possibly others. In effect, TfL has set a de facto regulatory standard and catalysed a surveillance arms race in the gig economy but have done so without the proper public scrutiny of a regulatory process.

Conclusion

Despite recent gains in the courts in various jurisdictions, the fundamental problems of precarity in the gig economy remain. Even where worker rights have been asserted, such as in the UK, there has been no wider enforcement by the government. This leaves workers with few alternatives to litigation, if they have the resources to do so. Worker status as a bottom rung classification still falls short for gig workers because it offers no protection from unfair dismissal. Failure to pay for waiting time as working time enables platforms to take advantage of the immediacy of availability to drive up customer response time while driving down worker earnings.

All of these problems are aggravated by the failure of platforms to respect the digital rights of workers. Our report shows woefully inadequate levels of transparency about the extent of algorithmic management and automated decision making workers are subject to in the gig economy. Workers are denied access to their personal data outright, are frustrated in their request or are simply given an incomplete return.

Here too we find the laws are weakly enforced and the scope of protection is insufficient. Article 22 protections from unfair automated decision-making provide escape options for employers who can claim superficial human review to rubber stamp unfair machine made decisions. The proliferation of profiling, generated by machine learning, can make it exceedingly difficult for workers to ever uncover, understand or test the fairness of automated decision-making relating to workplace fundamentals such as work allocation, performance management and disciplinary action.

Even where disclosures are made, we may only at first gain a one dimensional view of personal data processing, whereas to truly understand algorithmic management at work, we need to understand the interplay between separate algorithmic management functions.

The new proposed EU directive has made great strides in identifying important new protections for gig economy platform workers in Europe such as the presumption of employment and enhanced protections against unfair automated decision making. But misclassification will continue to challenge this process if rogue employers continue to hide true performance management decisions & intensive surveillance behind the label of anti-fraud prevention.

It takes time and money to access remedy in court, and precarious workers need more rapid solutions if they are to be effective at all. That is why workers must improve their bargaining power through organising and collective action. The ability of workers therefore to access and pool their data is a powerful force in organising yet to be properly tapped. When workers can better control their data, they will be better able to control their destiny at work.