c/o The Society of Authors
24 Bedford Row
London WC1R 4EH
Wednesday 28 February 2024

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

1. THE COMPLAINANTS

This complaint is made by Jim Killock.

Jim Killock is the Executive Director of the Open Rights Group, a digital rights campaigning organisation. It campaigns for a world in which each individual controls the data their digital lives create, decides who can use it and how, and where the public's rights are acknowledged and upheld.

2. OPEN RIGHTS GROUP

Open Rights Group (**'ORG'**) is a UK-based digital campaigning organisation working to protect rights to privacy and free speech online. ORG challenges threats to privacy by both the government through the surveillance of our personal communications and private companies, who use our personal data to increase their profits.

ORG is not-for-profit organisation with statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data. ORG is

mandated by Jim Killock to lodge this complaint on his behalf under Article 80(1) UK GDPR.[1]

Since 2022, ORG has worked with technical experts to investigate processing of personal data by the LiveRamp group, whose parent company is LiveRamp Holdings, Inc, registered in California. The LiveRamp group monitors hundreds of millions of individuals globally[2] and has offices and operates in the UK. LiveRamp is processing the personal data of millions of individuals in the UK. That is, it is both monitoring the behaviour of data subjects in the UK and its processing takes place in the context of an establishment in the UK. The ICO has jurisdiction to investigate LiveRamp's processing in accordance with Article 3 of the UK GDPR. Our investigation discloses serious concerns that this processing is not lawful.

3. LIVERAMP'S PROCESSING OF THE COMPLAINANTS' PERSONAL DATA

Following subject access requests, The Complainants learned that LiveRamp has processed their personal data[3] as part of its business operations (see section 5 below).

In light of ORG's investigation and what they now know about this processing, the Complainants believe it to be unlawful.

The Complainants are aware that the ICO normally expects data subjects to first seek resolution from the data controller before making a complaint. They have not done so in this because it would clearly be futile:

- The unlawful processing goes to the heart of LiveRamp's business model. There is no prospect of LiveRamp bringing it into compliance on the basis of an informal complaint from a data subject;
- Even were LiveRamp to offer remedies for the Complainants—such as deleting their data—this would not address the widespread unlawful processing which they are engaged in, and which greatly concerns the Complainants and calls for regulatory action.

[1] The mandates are in annex II.

[2] Citations for facts stated in this letter are included within the annexed Technical Report.

[3] See Annex III for copies of the relevant correspondence.

4. ORG'S INVESTIGATION

ORG's investigation involved the collation and analysis of extensive publicly-available information about LiveRamp—much of it provided by LiveRamp itself. ORG also carried out basic browser observations to observe—to the limited extent possible—how data moves between LiveRamp and other sites as individuals browse online. To carry this out ORG worked with Cracked Labs,[4] an independent research institute based in Austria which investigates the societal implications of information technology.

The Complainants are submitting the full report, drafted by Cracked Labs, to you now, as they believe the investigation demonstrates that LiveRamp has unlawfully processed the Complainants' personal data, and raises wider questions about the lawfulness of LiveRamp's processing.

5. LIVERAMP'S BUSINESS MODEL

LiveRamp's business involves the maintenance of vast databases of personal information, from postal addresses and phone numbers to email addresses and cookie identifiers. LiveRamp infers connections between these pieces of information, linking them with pseudonymous identifiers so that with just one piece of information —a device identifier or email address for example—a comprehensive identifying profile of an individual can be retrieved. Its databases may be thought of as private population registers.

LiveRamp sells this functionality to a wide range of online actors, allowing them to monitor individuals as they browse, and to communicate with other online actors about individuals—most particularly individuals whom they want to track, profile, advertise, and sell to. In this way LiveRamp's processing plays a major role in today's marketing surveillance ecosystem, since it facilitates ad-tech and behavioural advertising without the need for third party cookies. LiveRamp also enables data brokers to sell personal data about millions of people to data buyers, who can then further transmit records to other

[4] https://crackedlabs.org/en

companies, all while ensuring the commercial actors in the chain are talking about the same individuals.

LiveRamp's processing is complex and the way its business model works is opaque and difficult to understand for ordinary consumers including the Complainants. It means that individuals browsing online can be tracked and influenced in a personalised way without their realising it. Indeed, even where a person uses browsing behaviours that they might think protect them from being tracked—e.g. not logging into sites, or only providing partial address information—hey can be monitored and profiled in ways they would not expect, thanks to LiveRamp's processing.

6. UNLAWFUL PROCESSING AND THE NEED FOR REGULATORY ACTION

Bearing in mind ORG's investigation, the Complainants believe LiveRamp's processing of their personal data to have breached the UK GDPR in at least the following ways:

6.1 Lawful basis for processing (Articles 5(1)(a) and 6)

LiveRamp offers inconsistent information about its lawful basis for processing. Its UK privacy notice suggests it relies principally on its legitimate interests. Its French privacy notice suggests it relies heavily on the consent of data subjects.

To the extent it relies on legitimate interests, there is good reason to believe that data subjects' interests override those of LiveRamp. LiveRamp's interests are purely commercial. These must be balanced against the seriously privacy-invasive nature of its processing, which minutely tracks people's online and offline behaviour (such as changes of physical address) and invisibly exposes their personal information to hundreds of clients.

To the extent it relies on the consent of the data subjects it monitors through its databases, there is good reason to believe that consent is not *'freely given, specific, informed and unambiguous'* as required by the UK

GDPR. In particular this is because the complexity and scale of LiveRamp's processing means it cannot be properly understood by data subjects in order for their consent (which in any event is not collected by LiveRamp but by third parties) to be informed.

6.2 Data minimisation and retention (Articles 5(1)(c) and (e))

Even if LiveRamp had a lawful basis for its processing, its system is designed around the indiscriminate collection and processing of personal data which is out of all proportion to its objectives. For example

- For many individuals, many more data points than strictly 'necessary' will be collected – and retained for longer than necessary[2]—in order for LiveRamp to maximise its chances of creating useful links between apparently unconnected pieces of personal data. In line with the principle of accountability, LiveRamp should be able to articulate with specificity how much data it needs to process for its purposes rather than simply seeking to process the maximum amount possible.
- Pseudonymous identifiers will be generated by LiveRamp—and linked to a range of personal data—for individuals who are *never* searched for or targeted by LiveRamp's clients, making the processing by definition unnecessary, despite its intrusiveness and the risk it creates to the data subjects who LiveRamp profiles.
- When data is sent for 'matching' by LiveRamp's clients, up to 10 pseudonymous identifiers be returned, which may correspond to a number of individuals, entailing additional unnecessary processing of the non-target individuals' personal data.

6.3 Purpose limitation (Article 5(1)(b))

LiveRamp's business model depends upon the reuse of personal data that was collected in other contexts. The Technical Report describes how data collected in the course of individuals' ordinary browsing or other activities is uploaded to LiveRamp from both LiveRamp clients and 'paid match partners'. This data is reused by LiveRamp for the new

purpose of identifying individuals and enabling them to be tracked and targeted by (other) LiveRamp clients.

This secondary purpose is unlikely to be compatible—in many cases—with the purpose for which the data was originally collected For example, if a user logs into a website in order to complete a purchase and provides address information, it is not consistent with purpose limitation for a 'paid match partner' to send that address information along with the cookieID to LiveRamp for the purposes of future tracking of the user by an unknown number of other LiveRamp clients.

6.4 Security of processing (Article 5(1)(f))

LiveRamp's databases contain a huge amount of personal data about 10s of millions of UK data subjects. LiveRamp provides multiple routes through which clients can query these databases. The data is potentially sensitive (e.g. revealing individuals' location and marital status) and sometimes includes special category data engaging Article 9 of the UK GDPR. The system could easily be misused (e.g. by someone trying to confirm a known individual's new address where they have their email and last address).

It is not clear what, if any, controls are in place to monitor how the system is being used and whether it is being used exclusively as intended – i.e. for marketing and commercial targeting purposes. LiveRamp needs to "be able to demonstrate compliance with" the security of processing in accordance with Article 5(2) but appears unable to do so.

6.5 Transparency and fairness (Articles 5(1)(a) 13 and 14)

The scale and implications of LiveRamp's processing are likely to be unexpected for data subjects. They were unexpected for the Complainants:

- A typical data subject would not expect that after their first visit to a website where they do not login or provide any personal data, the operator of that site can—using LiveRamp's databases—track them

and make decisions about their browsing experience when they return—even on a different device.
- Nor would a data subject expect that by providing address information to one online service, they are contributing to a system which allows any LiveRamp client to 'talk to' up to hundreds of other LiveRamp clients about the data subject for the purposes of marketing.

LiveRamp does not appear to take sufficient steps to inform data subjects of its processing in a way that enables them to meaningfully understand it. And it did not do so in respect of the Complainants.

LiveRamp is processing the personal data of millions of data subjects in the UK beyond the Complainants. ORG's investigation suggests that much of this processing is unlawful.

This complaint is not intended as a comprehensive legal analysis of LiveRamp's processing. The scale and opacity of LiveRamp's processing makes it unrealistic for any individual complainant to fully investigate and legally analyse it. For this reason, it is also unrealistic for the Complainants to take civil legal action against LiveRamp, whose processing affects millions of data subjects.

We therefore urge you to use your powers under the UK GDPR to investigate the lawfulness of LiveRamp's processing, resolve the Complainants' complaints and, if necessary, take appropriate further regulatory action to protect the rights and freedoms of UK data subjects.