Wolfie Christl, Alan Toner, February 2024

Pervasive identity surveillance for marketing purposes

A technical report on personal data processing for LiveRamp's "RampID" identity graph system based on an analysis of software documentation with a focus on Europe

A report by Cracked Labs (crackedlabs.org), commissioned by Open Rights Group (openrightsgroup.org), February 2024.

Authors: Wolfie Christl, Alan Toner.

The research for this report was conducted in September 2023. Every effort has been made to ensure the accuracy of the texts in this report. The author and the publisher accept no liability in the case of eventual errors.

Contents

1. Introduction and overview

In recent years, a wide range of companies has started to monitor, track, and follow people in virtually every aspect of their lives. A vast landscape of data companies has emerged that consists not only of large players such as Google and Meta, but also thousands of other businesses from various industries that continuously share and trade digital profiles with each other. Companies have started to combine and link data from the web and smartphones with the customer data and offline information that they have been amassing for decades. Many businesses try to record and measure every interaction with a consumer, including on websites, platforms, and devices they do not control themselves. They can seamlessly collect rich data about their customers and others in real-time, enhance it with information from third parties, and utilize the enriched profiles for digital advertising, which is often based on real-time auctions of consumer profiles.[1] The lawfulness of many of these data practices under the GDPR is disputed and subject to ongoing debate and litigation.[2]

LiveRamp,[3] formerly known as Acxiom,[4] is a major player in this marketing data industry. As a consumer data broker, the company sells data about 700 million consumers globally from 150 data providers through its "data marketplace".[5] Perhaps more importantly, LiveRamp operates a massive identity surveillance system that assigns every person a proprietary identifier, which is tied to identifying attributes such as names, postal addresses, email addresses, phone numbers and digital IDs referring to browsers, smartphones and other devices. Its "AbiliTec" and "RampID" systems maintain and constantly update comprehensive identity records about whole populations: the address where they live, the devices they use, and people they share a household with. LiveRamp explains that "people are dynamic". Each time they "move houses, change jobs, switch phones, share computers, and upgrade their tech", this may create a new identity record in its systems. "Over time, each of these events builds a more complete picture of that person's identity".[6] LiveRamp's identity graph systems can be considered private population registers, and their identity databases and proprietary identifiers facilitate the exchange of personal data across databases and companies. Many businesses in the digital marketing industry utilize LiveRamp's identity surveillance technology to recognize, track, follow, profile and target people across the digital world and trade profile information about them. The company also promotes its identity graph systems as a solution to sell behavioral advertising "without third-party cookies".[7] LiveRamp is based in the US, listed at the NYSE and has offices in London and Paris.[8] As of 2023, LiveRamp "operates" in many countries across the planet including the UK, France, Germany, Belgium, Spain, Italy, Poland and Romania.[9]

This report investigates LiveRamp's identity surveillance technology and data practices that rely on it with a focus on Europe, France and the UK. It builds on previous research[10] and is largely based on a detailed analysis of software documentation available online. To a smaller extent, it relies on an analysis of promotional materials and legal documents such as privacy policies. The report represents a working document that aims to serve as evidence for the further investigation of LiveRamp's data practices by scholars, policymakers, journalists, privacy advocates and regulators. As a "technical report", it assumes some knowledge from readers about today's marketing data industry. The report documents a wide range of data practices:

- **Section 2** examines the basic functionality of LiveRamp's identity surveillance technology. It shows that LiveRamp maintains population-scale identity databases that contain comprehensive identity records about 700 million people globally, 45 million people in the UK and 25 million people in France. The AbiliTec identity graph links different "offline" identifiers to each other, including names, postal addresses, email addresses and phone numbers (section 2.1). The RampID system links digital identifiers to a person's AbiliTec record, including mobile device IDs, cookie IDs, connected TV IDs and other proprietary IDs (section 2.2). LiveRamp claims to have data about 14 billion devices globally. It rarely

[1] Christl, Wolfie (2017): Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. A Report by Cracked Labs, Vienna, June 2017. Online: https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[2] See e.g. https://www.iccl.ie/digital-data/, https://noyb.eu and https://www.forbrukerradet.no/out-of-control/
[3] https://liveramp.com
[4] https://www.mrweb.com/drno/news26864.htm [19.9.2023]
[5] https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [5.9.2023]
[6] See section 2.7
[7] https://liveramp.com/our-platform/authenticated-traffic-solution-ats/ [19.9.2023]
[8] https://d18rn0p25nwr6d.cloudfront.net/CIK-0000733269/218aac94-b9de-4932-838b-b5b55394b906.pdf
[9] https://docs.liveramp.com/connect/en/the-countries-liveramp-operates-in.html [19.9.2023]
[10] Christl, Wolfie (2017): Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. A Report by Cracked Labs, Vienna, June 2017. Online: https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

provides raw identifiers such as email addresses to its clients. Typically, companies send consumer records that contain identifying information to LiveRamp, which tries to find matching person records in its identity databases and then returns a pseudonymous "RampID" identifier that refers to a partial or full person record in the company's identity databases. LiveRamp's clients can utilize the RampID system to combine and link personal data across databases and exchange personal data across companies. They can utilize it to track website and mobile app users, recognize and profile people by "onboarding" entire customer databases and then transmit consumer records to adtech firms or large platforms for ad targeting and other purposes via LiveRamp's "Connect" platform (section 2.2.5). In order to maintain its identity graph databases (section 2.3) and constantly keep them updated, LiveRamp obtains and purchases identity data from "offline" data sources, "match partners" and other data providers (section 2.4). Several documents provided by LiveRamp describe how its clients can utilize the company's identity data to recognize, track and profile people across the digital world, buy and sell data, target them with ads and personalize websites, mobile apps and other services (section 2.5). LiveRamp's UK and French services privacy policies describe the legal justification of its data practices (section 2.6).

- **Section 3** further explores applications that rely on LiveRamp's identity surveillance technology. LiveRamp's "Connect" platform allows clients to "distribute" consumer records to Google, Facebook, large publishers, adtech firms and other data companies. Clients can utilize LiveRamp's identity data to transmit lists of RampIDs and other identifiers referring to persons with certain characteristics to third-party companies, referred to as "destinations", which link the transmitted data to their own databases that contain records about millions of people (section 3.1.1). Data brokers and other businesses can utilize LiveRamp's identity data and its "data marketplace" to sell consumer data to other companies, including in the UK and in France (section 3.1.2). RampIDs can serve as "universal identifiers" in the broader data and adtech industry. RampIDs are transmitted via the RTB bidstream in digital advertising in order to link and match personal data across a large number of publishers, advertisers and adtech intermediaries. This occurs 60 billion times a day, according to LiveRamp (section 3.2). Google utilizes RampIDs as "join keys" between its advertising clients' data and its own massive data sets (section 3.2.4). Via LiveRamp's "Authenticated Traffic Solution" (ATS) product, publishers such as websites, mobile apps and other digital services can turn their users' email addresses into pseudonymous RampIDs, which can then be transmitted via the RTB bidstream in order to enable adtech firms and advertisers to profile and target these users. ATS introduces the concept of "identity envelopes", which contain encrypted RampIDs. Identity envelopes can be decrypted and linked to other identifiers in different ways (section 3.3).
- **Section 4** summarizes some of the findings in this report and provides concluding remarks. LiveRamp's identity surveillance technology relies on pseudonymization that is claimed to be "one way". The company rarely or never provides raw identifiers such as names, postal addresses, email addresses or phone numbers to other firms. Instead, clients and partners can send consumer records that contain identifying information from different sources to LiveRamp, which returns pseudonymous RampIDs that can be utilized to combine and link consumer records across databases. A data broker can, for example, utilize RampIDs to sell personal data about millions of people to data buyers, who can then utilize RampIDs to transmit the records to third-party companies who match these records to billions of consumer records they process themselves. While RampIDs are formally "vendor-specific", many of LiveRamp's clients are themselves data intermediaries who process personal data on hundreds of millions of people on behalf of many of their own clients. As such, RampIDs can be utilized to exchange personal data across many actors. In addition, RampIDs specific to one company can be converted into RampIDs specific to another company. While this process is governed and controlled by LiveRamp, the findings in this report suggest that adtech intermediaries such as SSPs and DSPs can utilize this "translation" process across vendor-specific RampIDs. This translation process also facilitates the exchange of personal data across many actors.
- Each time a company utilizes a RampID to link and match personal data, it processes a pseudonymous identifier that is tied to a person's partial or full identity record maintained by LiveRamp. As a result, pseudonymization turns from a measure that protects data subjects from re-identification and personal data linkage across contexts to a more powerful means to join personal data across databases and companies than a name. The findings in this report suggest that LiveRamp's "Authentic Traffic Solution" (ATS) product and its encrypted "identity envelopes" may be considered a thin compliance layer over the RampID system, just as the RampID system may be considered a thin compliance layer over LiveRamp's "offline" identity databases that contain names, postal addresses, email addresses and phone numbers. LiveRamp's intrusive data practices may disproportionally affect the rights and freedoms of hundreds of millions of people

in the UK, France and other countries, and raise questions about the lawfulness of LiveRamp's data practices under the GDPR and UK data protection legislation.

Limitations. This report investigates LiveRamp's data practices largely based on publicly available information provided by the company. This includes software documentation and promotional materials, which might be ambiguous and incomplete. Every effort has been made to accurately interpret these corporate sources, but we cannot accept any liability in the case of eventual errors. While LiveRamp's software documentation consists of several thousands pages and provides comprehensive information about how its clients can utilize the company's systems, it remains largely unclear how clients and other organizations actually implement and customize the functionality provided by these systems.

2. LiveRamp's identity graph systems

LiveRamp maintains a variety of identity databases that contain identifying information referring to hundreds of millions of people, the places and addresses they live, and any people they share a household with. This population-scale identity surveillance system was created by Acxiom in the late 1990s and is now operated by LiveRamp. For decades, it has been called "AbiliTec".[11]

AbiliTec identity graph. LiveRamp describes its AbiliTec identity graph as "a vast, multi-sourced historical identity graph containing over 40 years of consumer contact information from over 150 data sources, including over 4.5 billion name and postal records, over 1.1 billion email addresses, and over 600 million phone numbers".[12] When clients send identifying information such as names, postal addresses, email addresses or phone numbers to LiveRamp, the Abilitec systems tries to match this information to existing records and returns one or several pseudonymous AbiliTec IDs referring to an individual consumer, a household or a place/address. Clients can the use these identifiers to match or exchange personal data across different databases. The AbiliTec "offline" identity graph is the basis for LiveRamp's RampID system that covers a wider range of digital identifiers and use cases. According to LiveRamp's UK and French websites, the company has "offline" identity data about 45 million people in the UK and 25 million people in France.[13]

RampID identity graph. In 2016, Acxiom (now LiveRamp) created a second "online" identity surveillance system it initially called "IdentityLink".[14] It was renamed to "RampID" in 2021.[15] On the one hand, the RampID system expands the scope of identifying information that is being processed into the digital space, covering digital identifiers such as cookie IDs, mobile device IDs, connected TV IDs and other proprietary IDs. On the other hand, the RampID system allows companies to query and utilize identity data maintained in LiveRamp's "offline" AbiliTec identity graph.

LiveRamp states in a recent annual report filed to the U.S. Securities and Exchange Commission (SEC) that it offers "multi-sourced insight into approximately 700 million consumers worldwide" through its "data marketplace".[16] As the company's data marketplace relies on its identity graph, this suggests that LiveRamps's identity graph contains person records about 700 million consumers globally.

LiveRamp's "clients" and "partners". LiveRamp often uses the terms "clients" and "partners" as synonyms. Sometimes, "partners" appear to be a subset of "clients".[17] In any case, LiveRamp has very different business relationships with different kinds of companies. Some companies utilize LiveRamp's identity surveillance technology to link data about their customers across databases. Others contribute data to LiveRamp's identity graph. Yet others may be powerful intermediaries in the data industry themselves, from platforms to adtech firms to data brokers. The term "partner" may refer to LiveRamp's business relationships with intermediaries that provide data services to many clients themselves.[18] In this report, the term "LiveRamp client" generally refers to companies LiveRamp has business relationships with.

---

[11] See Christl (2017): Corporate Surveillance in Everyday Life, p. 42, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[12] https://developers.liveramp.com/abilitec-api/docs/the-abilitec-identity-graph-1 [5.9.2022]
[13] See section 2.1
[14] https://www.prnewswire.com/news-releases/liveramp-launches-identitylink-to-power-people-based-marketing-for-brands-300343299.html
[15] https://liveramp.com/blog/identitylink-now-rampid/ [5.9.2023]
[16] https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [5.9.2023]
[17] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]
[18] https://partner-directory.liveramp.com/ [5.9.2023]

AbiliTec vs. RampID identity graphs. The following graphic, dated 2019, shows how LiveRamp explains the relationship between its "offline" and "online" identity graph systems:[19]

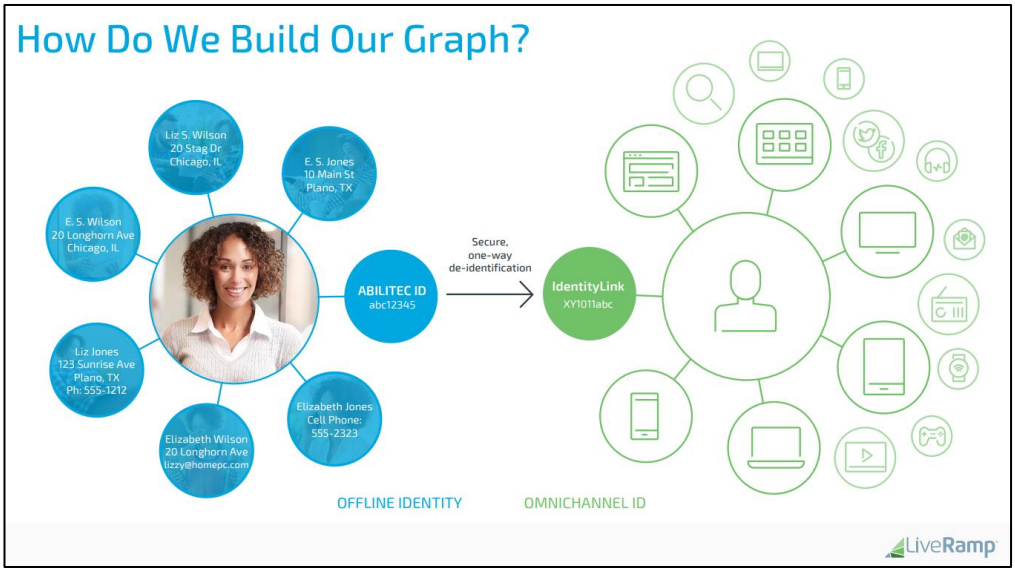


Figure 1 © LiveRamp

The above graphic suggests that LiveRamp maintains AbiliTec IDs that refer to names, postal addresses, phone numbers and email addresses, as well as IdentityLink IDs (now RampIDs) that refer to all kinds of pseudonymous identifiers in the digital space. The former can be "translated" into the latter by "one-way de-identification". As section 2.2 shows, this still potentially allows thousands of companies to send names, postal addresses or email addresses to LiveRamp, receive the corresponding RampIDs, and then match them with records that are also linked to RampIDs from many other companies.

The following graphic, dated 2019, also shows how LiveRamp explains the relationship between its two identity graphs:[20]

Figure 2 © LiveRamp

[19] p. 9, https://www.ai-expo.net/northamerica/wp-content/uploads/sd-uploads/PDF%204%20APPLIED%20AI/11.50_Liveramp.pdf [5.9.2023]
[20] LiveRamp Form 10k for the fiscal year ended March 31, 2019: https://www.sec.gov/Archives/edgar/data/733269/000073326919000022/ramp-20190331.htm

The above graphic shows how a client can send customer data to LiveRamp via the "Connect" system. When LiveRamp finds an existing person record in its AbiliTec "offline" identity graph, it creates a pseudonymous IdentityLink ID (now RampID). The pseudonymous RampID identifier can then be utilized to seamlessly process, match and transmit personal data about this person across different databases, companies, browsers and devices that is linked to the same RampID.

2.1 The "AbiliTec" system

LiveRamp describes the AbiliTec identity graph as a "vast, multi-sourced historical identity graph containing over 40 years of consumer contact information from over 150 data sources".[21] It is "rebuilt each month with updated data from data sources". LiveRamp states that the "following information is stored in the AbiliTec Identity Graph for linking":[22]

- "Consumer names and name variations"
- "Postal addresses"
- "Email addresses"
- "Phone numbers"
- "Consumer associative data, such as gender or year of birth (used to build people and household formations)"
- "Internal metadata, such as frequencies, classifications, and thresholds for making linking decisions"

LiveRamp claims that its identity graph contains data on **25 million people in France**[23] and **45 million in the UK**[24] and is based on "100+ sources for offline, historical information".[25] LiveRamp's "matching technology" based on the AbiliTec identity graph "recognizes name and touchpoint variations of an individual occurring in company systems over time and brings together similar and what would appear to be dissimilar representations. These records are each assigned a persistent AbiliTec identifier".[26]

As the next sections show, LiveRamp rarely returns raw directly-identifying information to its clients. Usually, it provides pseudonymous identifiers that refer to raw records stored in LiveRamp's databases. Clients send identifying information to LiveRamp and can then use the pseudonymous identifiers returned by LiveRamp for all kinds of purposes.

2.1.1 AbiliTec basics

The AbiliTec system provides the following key functionality:

- Clients can send one or many records that contain identifying information such as first name, middle name, last name, street address, city, zip code, phone numbers and/or email addresses to LiveRamp.[27]
- The AbiliTec system uses sophisticated mechanisms (e.g. the "match cascade") to find existing records that match the provided data about the corresponding individual and then returns so-called "AbiliTec Links" to clients. The returned "AbiliTec Links" can be identifiers referring to individuals ("AbiliTec ConsumerLink"), households ("AbiliTec HouseholdLink") and places/addresses ("AbiliTec AddressLink").[28]

[21] https://developers.liveramp.com/AbiliTec-api/docs/the-AbiliTec-identity-graph-1 [5.9.2023]
[22] https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [5.9.2023]
[23] "L'Identity Graph de LiveRamp est le plus grand graph déterministe sur l'open internet, avec plus de 25 millions de consommateurs représentés en France", "Atteignant plus de 25 millions de personnes appariées en ligne, notre graph d'identité fournit le plus grand graph déterministe disponible à des fins commerciales pour identifier des individus (sous forme identifiée et pseudonyme)", "Cibler plus de 25 millions de personnes actives en ligne", "Plus de 100 sources d'informations historiques hors ligne" https://liveramp.fr/notre-plateforme/identity-graph/ [22.6.2022], https://web.archive.org/web/20220820055217/https://liveramp.fr/notre-plateforme/identity-graph/
[24] "LiveRamp's identity graph is the largest deterministic graph on the open internet, with more than 45 million consumers represented in the UK", "Reaching over 45 million matched UK people online, LiveRamp provides the largest deterministic identity graph available for commercial use for identifying individuals", "Reaches more than 45 million active people online across the UK" https://liveramp.uk/our-platform/identity-graph/ [22.6.2022], https://web.archive.org/web/20220613155152/https://liveramp.uk/our-platform/identity-graph/
[25] Ibid.
[26] https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [5.9.2023]
[27] https://developers.liveramp.com/AbiliTec-api/reference/match-single-transaction-calls [5.9.2023]
[28] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]

An AbiliTec Link identifier that is returned to a client consists of 16 alphanumeric characters. The first 4 characters are **client-specific**, i.e. different clients receive identifiers that look distinct but refer to the same individual, household or place/address.[29] LiveRamp also refers to "AbiliTec Links" as "AbiliTec IDs", which are "identifiers that are tied to a record in the AbiliTec Identity Graph. They allow [clients] to identify and consolidate records across multiple systems".[30]

2.1.2 Individual, household and place/address IDs

LiveRamp describes three types of AbiliTec IDs:[31]

- A "ConsumerLink" identifier "represents an individual", according to LiveRamp. It is "unique to each individual".
- A "HouseholdLink" identifier "represents adults living together at the same location who exhibit a persistent relationship", a "group of individuals that share a primary residence and likely make purchase decisions as a unit".
- An "AddressLink" identifier "represents a site or physical location". It is a "unique identifier for a physical business or residential address".

2.1.3 "Maintained" and "derived" IDs

LiveRamp returns either "maintained" or "derived" AbiliTec IDs:[32]

- LiveRamp returns **"maintained" IDs** to a client if an existing record in the AbiliTec identity graph perfectly matches the input data sent to LiveRamp before. These IDs are "maintained in the graph, and so are persistent".
- If LiveRamp didn't find an existing record in the AbiliTec identity graph based on the input data sent, it returns a **"derived" ID** to the client, which is "algorithmically derived" from the input data.
    - The same input data consistently leads to the same "derived" ID. If a client, for example, sends data about "John Doe, 9398 Chester Road, London, johndoe@gmail.com" and LiveRamp doesn't find an existing record in its database that fits, it will return a "derived" ID for this person, and it will always return the same "derived" ID again when sent the same input data. In this way, clients can use the "derived" AbiliTec ID as a key in their databases and handle it as if it was a "maintained" ID.
    - Because "new data content is added to the AbiliTec Identity Graph on an ongoing basis", input data that returns "derived" IDs may return "maintained" IDs at some point in the future.
    - LiveRamp may return "derived" individual IDs, "derived" household IDs, and "derived" place/address IDs.
    - There can be collisions, LiveRamp may sometimes return the same derived ID for different input data.

2.1.4 How to query the AbiliTec system – "match" vs. "lookup"

LiveRamp provides two different ways for clients to query the AbiliTec system via the "AbiliTec API":[33]

- When using the **"Match"** function, clients send plaintext/raw personal data such as name, address, email and phone number to LiveRamp. LiveRamp applies "data normalization" and "approximate matching" (to address "misspellings, JR/SR conflicts, name swaps, and address formatting variations") and then takes the input data through a sequence of matching steps (the "match" cascade") utilizing various attributes of the input data "until a match to a maintained AbiliTec identifier is found. If no maintained AbiliTec ID is found after all steps of the match cascade are performed, a derived AbiliTec ID is returned".[34]
    - The AbiliTec API docs contain detailed information about the types of data that clients can send to the "Match" API endpoint, as well as about the types of data returned to them.[35] Input data can include:[36]
        - Name, street address, zip code, email address, phone number or a combination of these attributes such as "name + zip", "name + email" or "name + phone".

[29] Ibid.
[30] https://developers.liveramp.com/AbiliTec-api/docs/the-types-of-data-that-can-be-returned [5.9.2023]
[31] https://developers.liveramp.com/AbiliTec-api/docs/AbiliTec-identifiers [5.9.2023], https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[32] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[33] https://developers.liveramp.com/AbiliTec-api/ [11.9.2023]
[34] Ibid.
[35] https://developers.liveramp.com/AbiliTec-api/reference/match-single-transaction-calls [6.9.2023]
[36] Ibid.

- LiveRamp can return **up to 10 AbiliTec IDs** including individual, household and place/address IDs. The first ID returned may, for example, be associated with the name, address and zip code sent to LiveRamp, the second with the name and phone number sent, and the third with the name and the email address sent. The first AbiliTec IDs returned corresponds to the best match.[37]
- Each returned record that contains AbiliTec IDs also contains **match metadata**, including:[38]
  - "Match components": a list of the input attributes that contributed to the match, e.g. "name, zip" when the returned AbiliTec ID matched name and zip
  - "Distinct match": indicates that the returned AbiliTec ID corresponds to exactly one distinct record in the AbiliTec identity graph
  - "Match confidence": numeric value indicating LiveRamp's level of confidence that the returned AbiliTec ID actually matches the input data
  - "Name match integrity": indicates whether part or all of the major name components matched the input data

- The **"Lookup"** function, in contrast, "does not use a match cascade. LookUp only returns exact matches, and it does not perform any approximate matching on inputs, which allows it to rapidly look up exact matches in the graph".[39] The Lookup function returns a single "maintained" AbiliTec ID record. If a corresponding maintained record is not found in the AbiliTec identity graph, it returns a "not found" message.[40]
  - The AbiliTec API docs contain detailed information about the types of data clients can send to the "Lookup" API endpoint, as well as about the types of data returned to them by LiveRamp.[41] Input data can include:[42]
    - Email address hashed with MD5, SHA1 or SHA256
    - Phone number hashed with SHA1
    - Combinations of name+email, name+phone, name+zip or others, hashed with SHA1
  - The "Lookup" function only accepts hashed versions of the input data. Clients can use the "Lookup" function for "transcoding" (see below) and "hashed entity matching", i.e. they can link records that contain personal data maintained in different databases with each other.[43]

2.1.5 Further details about the AbiliTec system

2.1.5.1 Exchanging AbiliTec IDs across clients

While an AbiliTec ID is always specific to a certain client, the "Lookup" function can also help clients to convert/transform an AbiliTec ID specific to one client to an AbiliTec ID specific to another client. LiveRamp refers to this process as "transcoding" the AbiliTec ID from one client "domain" to another client "domain", which will be allowed only "if the client has permission from the owner of that domain and that permission has been shared in written form to LiveRamp".[44]

An older version of the AbiliTec API docs contains additional details about this **"transcoding" process**.[45] According to these docs, a client can convert an AbiliTec ID into an AbiliTec ID "encoded" for another partner/client ("native to other"). The client can also encode an AbiliTec ID received from another partner/client into an AbiliTec ID encoded for itself ("other to native").[46] The newer version of the AbiliTec API docs does not include this page anymore. It is not clear whether this functionality is no longer available, whether it is still available but not included in the publicly available docs, or whether LiveRamp's RampID system has perhaps replaced this functionality. It is almost certain that LiveRamp still provides functionality to convert AbiliTec IDs specific to a certain client to AbiliTec IDs specific to another client.

---

[37] https://developers.liveramp.com/AbiliTec-api/docs/the-match-endpoint [6.9.2023]
[38] https://developers.liveramp.com/AbiliTec-api/docs/the-match-endpoint [6.9.2023], https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[39] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[40] https://developers.liveramp.com/AbiliTec-api/docs/the-lookup-endpoint [6.9.2023]
[41] https://developers.liveramp.com/AbiliTec-api/docs/the-lookup-endpoint [6.9.2023], https://developers.liveramp.com/AbiliTec-api/reference/lookup-endpoint-single-transaction [6.9.2023], https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[42] Ibid.
[43] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[44] Ibid.
[45] https://developers.liveramp.com/AbiliTec-api/v1.1/docs/transcoding-endpoint [6.9.2023]
[46] Ibid.

2.1.5.2 Additional metadata about postal addresses, email addresses and phone numbers

When sending raw names and addresses, hashed email addresses or other identifying information to LiveRamp and then receiving maintained or derived AbiliTec IDs on individuals, households and places/addresses, LiveRamp can provide "additional insight" into the "client's customer data", which can provide "powerful signals for making decisions based on AbiliTec links or for building applications on AbiliTec link data":[47]

- **Contact flags:** When sending a certain postal address, email address or phone number to LiveRamp, it can return information about whether this postal address, email address or phone number is the "best contact" for that individual.[48] Clients can, for example, send different postal addresses and phone numbers stored in their own consumer database to LiveRamp and learn which one to use for this individual.
- **Email insights:** When sending an (hashed) email address to LiveRamp, it can return information about whether the email address owner has recently used this email, including the date and time the person clicked on a link in an email tracked by LiveRamp.[49] As such, clients can learn whether an email address is in active use. This "signal relies on specific deterministic signals from a small subset of LiveRamp match data contributors".[50]

2.1.5.3 ID graph data beyond names, postal addresses, phone numbers and email addresses

The previous paragraphs show that LiveRamp provides AbiliTec IDs and supplemental metadata to clients. In addition, LiveRamp's docs suggest that the AbiliTec system also processes "[c]onsumer associative data, such as gender or year of birth (used to build people and household formations)".[51] The docs, as available in April 2022, suggested that "location data such as the latitude or longitude and the IP address" and even "the sum of the last 4 digits of the social security number"[52] can be sent to LiveRamp to "improve matching accuracy".[53] These details have since been removed from the corresponding page in the docs[54] but they still mention LiveRamp's use of "location data to improve matching".[55] LiveRamp's UK services privacy policy describes that the company collects personal attributes like "marital status, title, date of birth, and gender" and other "attributes (such as demographic data)".[56] The French service privacy policy policy only mentions date of birth.[57]

2.1.5.4 "Householding algorithms"

Generally, LiveRamp appears to process personal data for the purpose of linking individuals to households. It states to "define users as being in the same household if they reside at the same address and show a persistent relationship".[58] It explains that "[s]eparate touchpoints of PII are linked to households via AbiliTec's householding algorithms. The algorithm puts individuals into households if they are seen consistently living together over time. There is no requirement for individuals to have the same last name or have a specific relationship (e.g. married). For example, long time roommates who keep moving together are likely to be grouped into the same household".[59]

2.1.5.5 Disclosing hashed email addresses to other companies

Parts of the docs suggest that LiveRamp also directly discloses email addresses to other companies rather than merely pseudonymous AbiliTec IDs. LiveRamp offers, for example, to increase the match rate with "Google Customer Match" by

[47] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[48] https://developers.liveramp.com/AbiliTec-api/docs/contactflags-bundle [6.9.2023]
[49] https://developers.liveramp.com/AbiliTec-api/docs/emailinsights-bundle [6.9.2023]
[50] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]
[51] https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [5.9.2023]
[52] Perhaps in the US only?
[53] https://developers.liveramp.com/retrieval-api/docs/data-you-can-send [14.4.2022]
[54] https://developers.liveramp.com/rampid-api/docs/data-you-can-send [6.9.2023]
[55] https://developers.liveramp.com/rampid-api/docs/data-you-can-send [6.9.2023], https://developers.liveramp.com/AbiliTec-api/docs/the-types-of-data-you-can-send [6.9.2023]
[56] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]
[57] https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]
[58] https://docs.liveramp.com/connect/en/precision-levels.html [6.9.2023]
[59] https://docs.liveramp.com/connect/en/rampid-methodology.html [6.9.2023]

"leveraging" its "Identity Graph to add additional emails" to data uploaded by clients.[60] As such, clients can send email addresses or other identifying information to LiveRamp, which in turn retrieves additional email addresses linked to the same person from its AbiliTec system and sends these additional email addresses in hashed format to Google.

2.1.6 AbiliTec use cases

Even though the AbiliTec identity graph does not return "understandable" identity information such as names or email addresses to LiveRamp's clients but usually pseudonymous AbiliTec IDs on individuals, households and places/addresses, it is a powerful identity surveillance system. Companies can convert scattered identifying information from different sources into AbiliTec IDs, use these IDs to join and combine other personal data that is linked to this identifying information, and learn additional metadata about this identifying information from LiveRamp's AbiliTec identity graph.

LiveRamp describes how clients can use the AbiliTec system to "unify data" (e.g. "unify PII-based records from a wide range of sources", "unite fragments of customer records … to a single record", "keep customer data fresh and up-to-date"), "expand records" (e.g. "validate connections between customer touchpoints", "add household and place dimensions"), "enrich identity" (e.g. use it to enrich customer records "with data attributes from leading third-party data providers") and to "improve data mobility and interoperability" (e.g. prepare individual and household data for "onboarding" and "online activation").[61]

Several charts in another help document provided by LiveRamp describe some use cases that exploit the limited capabilities of the AbiliTec system in a sophisticated way. They show, for example, how clients can use AbiliTec identifiers and match metadata returned by LiveRamp to unify customer files with different identifiers, merge duplicate records or validate data on customer "touchpoints":[62]

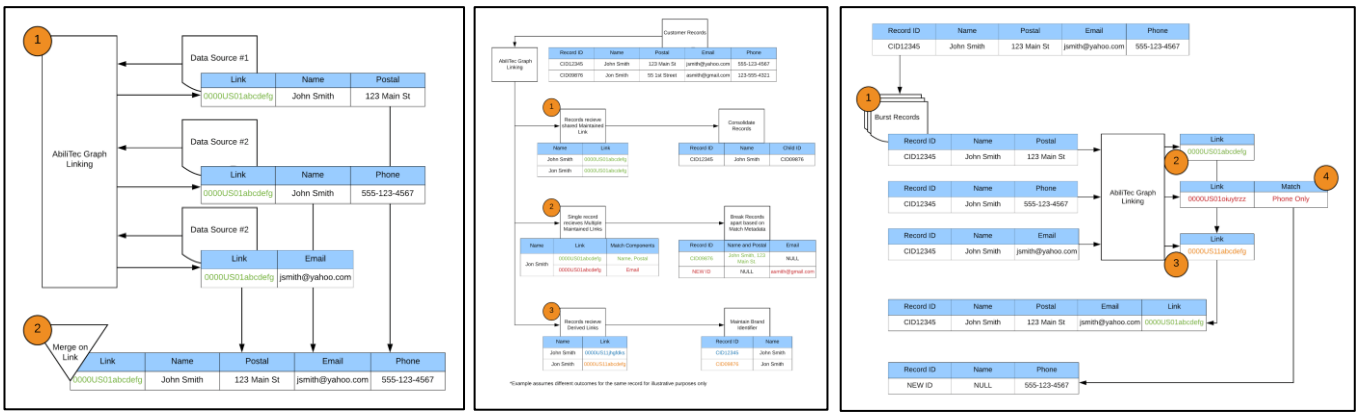


Figure 3 © LiveRamp

Most important, the "RampID" identity system, as detailed in section 2.2, relies on the AbiliTec identity graph.

2.1.7 (Pseudo) compliance measures

LiveRamp applies several design principles and measures that help to make its AbiliTec system look more compliant:

- At a basic design level, the fact that LiveRamp (almost) never provides raw identifying information such as names, postal addresses, email addresses or phone numbers to clients, but lets everyone "deal" with personal data only using its pseudonymous AbiliTec IDs as identity keys, is a powerful measure. It makes some use cases more complicated and has the potential to distract from the fact that AbiliTec IDs can still be used to combine and share all kinds of personal data associated with different personal identifiers across contexts, systems, databases and companies at scale. LiveRamp states that it "is not possible to determine an individual's name or address by looking at the ConsumerLink"[63], which is

[60] https://docs.liveramp.com/connect/en/distribute-first-party-data-to-google.html [5.9.2023], https://docs.liveramp.com/connect/en/announcing-the-ability-to-deliver-first-party-data-to-dv360-through-google-customer-match--9-2-21-.html [5.9.2023]
[61] https://docs.liveramp.com/identity/en/driving-value-with-AbiliTec.html [6.9.2023]
[62] https://docs.liveramp.com/identity/en/using-AbiliTec-identifiers.html [6.9.2023]
[63] https://docs.liveramp.com/identity/en/AbiliTec-components.html [5.9.2023]

probably true. Nevertheless, this measure doesn't prevent companies from retrieving individual-level AbiliTec IDs that correspond to identifying information collected in different contexts and then acting on that.

- LiveRamp uses client-specific AbiliTec IDs. This is a technical security measure and theoretically helps to prevent unauthorized actors from making any use of the IDs. However, LiveRamp almost certainly still provides ways to convert/translate AbiliTec IDs specific to one client to AbiliTec IDs specific to another client, as detailed in the previous paragraphs. As converting/translating RampIDs across clients is certainly possible (see section 3.2), LiveRamp's clients and partners can use the RampID system (that relies on the AbiliTec system) to link personal data across companies.
- LiveRamp explains that the "AbiliTec Identity Graph is non-discoverable, meaning the data stored within it has been obfuscated and is not retrievable by any client, third party, or any LiveRamp associate who is not directly involved in its development or support. It is only used for analysis to create and maintain AbiliTec IDs".[64] LiveRamp also states that "[b]efore a new data source is added to the identity graph, LiveRamp carefully vets the source to ensure compliance, quality, reliability, contribution value, and sustainability of the data. Additionally, LiveRamp continuously monitors existing sources to ensure the quality of those sources" … "After we cleanse the data and once we ensure that it meets the threshold for identifying a person, we associate those touch points with an AbiliTec ConsumerLink".[65] While both statements refer to technical and organizational measures, the details remain unclear. In any case, LiveRamp admits that AbiliTec IDs rely on data that "meets the threshold for identifying a person".[66]

2.1.8 Europe, UK, France?

Many of the available docs about the AbiliTec system refer to the US, which is where Acxiom initially created the technology. LiveRamp's websites and other docs suggest that it maintains AbiliTec data at least in the UK and France. It is, however, not entirely clear which functionality is provided in European countries:

- LiveRamp's AbiliTec help docs mention that clients can utilize an "international graph" outside the US.[67] It is not clear whether such an "international graph" differs from LiveRamp's AbiliTec graph in the US.
- LiveRamp's UK and French website rarely mention the term "AbiliTec" prominently, but they do. LiveRamp UK promotes the AbiliTec API on its website.[68] Until 2022, LiveRamp's UK website promoted "AbiliTec" as a "patented resolution technology" and a "patented recognition-linking technology", which helps clients "resolve personal data across enterprise data sources, unifying disparate points of data in [their] system that belong to the same individual to deliver a better customer experience". LiveRamp's "patented algorithms incorporate signals" that allow clients to "understand relationships between people, places, and household formations".[69] LiveRamp's French website contained similar sentences until 2022.[70] Both websites describe that other technologies provided by LiveRamp are "leveraging LiveRamp's AbiliTec offline resolution technology".[71]
- LiveRamp's docs, including the docs about the company's RampID system, often refer to the "AbiliTec" identity graph and "AbiliTec IDs". One page in the docs describes the "RampID", which "represents an individual", as a "pseudonymized version of an AbiliTec Person ID which is based on PII".[72] Another page states that "AbiliTec Links can be directly translated to RampIDs, creating a deterministic offline-to-online view of an individual".[73] Many doc pages describe how LiveRamp uses names, postal addresses, email addresses and phone numbers stored in its identity graph to provide its services, from the RampID system[74] to its "onboarding" services.[75]

[64] https://developers.liveramp.com/AbiliTec-api/docs/the-AbiliTec-identity-graph-1 [5.9.2022]
[65] Ibid.
[66] Ibid.
[67] https://docs.liveramp.com/identity/en/using-AbiliTec-identifiers.html [6.9.2023]
[68] https://liveramp.uk/developers/industry/platform/ [6.9.2023]
[69] https://liveramp.uk/our-platform/identity-infrastructure/ [22.6.2022]
[70] https://liveramp.fr/notre-plateforme/infrastructure-identite/ [22.6.2022]
[71] https://liveramp.uk/blog/answers-to-your-google-announcement-questions/ [6.9.2023], https://liveramp.fr/blog/annonces-de-google-toutes-les-reponses-a-vos-questions/ [6.9.2023]
[72] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[73] https://docs.liveramp.com/connect/en/rampid-methodology.html [6.9.2023]
[74] Ibid.
[75] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]

- LiveRamp's UK and French websites often discuss "offline" data and "offline identity resolution" without mentioning the term "AbiliTec".[76] As described in the opening paragraphs of section 2.1, the UK and French websites stated in 2022 that LiveRamp has data on 25 million people in France[77] and on 45 million people in the UK[78] from "100+ sources for offline, historical information".[79]
- LiveRamp's UK and French services privacy policies also discuss "offline" data a lot. Both state that LiveRamp collects names, birthdates, postal addresses, email addresses and phone numbers. While the UK policy states that "offline information collected from Database Providers will be retained while there's a continuing need to keep it for the applicable purposes", the French policy states that LiveRamp retains the processed personal data for 2 years from the last interaction with the data.[80]
- It appears that LiveRamp is phasing out out the "AbiliTec" brand name. While it is not clear whether the AbiliTec API described in section 2.1.4 is fully available to external clients in the UK and in France, the findings in section 2.1 suggest that LiveRamp generally collects, retains and uses extensive "offline data" including names, postal addresses, phone numbers and email addresses in Europe.

2.2 The "RampID" system and LiveRamp "Connect"

In 2016, Acxiom (now LiveRamp) created a second "online" identity surveillance system accompanying the AbiliTec identity graph. Initially called "IdentityLink",[81] it was renamed "RampID" in 2021.[82] The term "RampID" appears to refer both to the RampID system and the pseudonymous RampID identifier it relies on.

The RampID system mirrors several concepts from the AbiliTec system. It also creates "maintained" and "derived" RampIDs for both individuals and households. As this section shows, LiveRamp's clients, websites, mobile apps and other digital services can send identifying information to LiveRamp and receive pseudonymous RampIDs that match existing records in LiveRamp's AbiliTec and RampID identity graph systems.

AbiliTec and RampID identity graphs. LiveRamp refers to the AbiliTec system as the "PII-based offline identity graph"[83] and to the RampID system as the "online identity graph".[84] While the AbiliTec system focuses on names, postal addresses, email addresses and phone numbers, the RampID system links these attributes to digital identifiers referring to browsers (cookie IDs), devices such as smartphones or smart TVs (device/advertising IDs) and user/customer accounts at different websites, platforms and services ("custom IDs").[85] Both systems are deeply intertwined. Sometimes the company just uses the term "LiveRamp identity graph" to refer to both systems.[86]

The term "RampID" refers to a pseudonymous identifier, which LiveRamp defines as follows:

- A RampID "represents an individual".[87] It is LiveRamp's "people-based ID".[88]

[76] See e.g. https://liveramp.uk/our-platform/cloud/, https://liveramp.uk/our-platform/website-personalisation/, https://liveramp.uk/marketing/, https://liveramp.fr/marketing/, https://liveramp.fr/mesure-marketing/ [6.9.2023]
[77] https://liveramp.fr/notre-plateforme/identity-graph/ [22.6.2022], https://web.archive.org/web/20220820055217/https://liveramp.fr/notre-plateforme/identity-graph/
[78] https://liveramp.uk/our-platform/identity-graph/ [22.6.2022], https://web.archive.org/web/20220613155152/https://liveramp.uk/our-platform/identity-graph/
[79] Ibid.
[80] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023], https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]
[81] https://www.prnewswire.com/news-releases/liveramp-launches-identitylink-to-power-people-based-marketing-for-brands-300343299.html
[82] https://liveramp.com/blog/identitylink-now-rampid/ [5.9.2023]
[83] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[84] https://docs.liveramp.com/connect/en/liveramp-data-security-overview.html [6.9.2023]
[85] See section 2.2.4
[86] https://developers.liveramp.com/rampid-api/docs/rampids [6.9.2023]
[87] Ibid.
[88] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]

- RampIDs are “pseudonymous identifiers that are tied to a record in the LiveRamp identity graph”. They allow clients to “identify and consolidate records across multiple systems”.[89] The RampID is “LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph”.[90]
- LiveRamp can “convert” an AbiliTec ID “into a pseudonymous, universal identifier called a RampID”.[91] AbiliTec IDs “can be directly translated to RampIDs, creating a deterministic offline-to-online view of an individual. Via this translation, any offline or online data can be matched to the same RampID space”.[92] A RampID is a “pseudonymized version of an AbiliTec ID, which is based on PII”.[93]

“Anonymous identifiers” and “PII”. Until recently, the terminology used by LiveRamp was misleading or could even be considered as deceptive. LiveRamp used to inaccurately refer to the RampID as an “anonymous identifier”[94], an “anonymized version of an AbiliTec Person ID” and an “anonymous, universal identifier”.[95] LiveRamp now accurately describes the RampID as a “pseudonymous identifier”. It appears that the company has now replaced many occurrences of the terms “anonymous” and “anonymized” in the docs with the terms “pseudonymous” and “pseudonymized”. In contrast to anonymized data, pseudonymized data is clearly personal data under the GDPR. LiveRamp now also emphasizes that “personally identifiable information” (PII) refers to “directly identifiable data” in the EU and UK.[96] LiveRamp still often uses the term “PII” in the docs. In most cases, this refers to names, postal addresses, email addresses and phone numbers.[97]

Figures 1 and 2 in section 2, as well as the following chart,[98] provide an overview of how LiveRamp sees and promotes its AbiliTec and RampID systems:

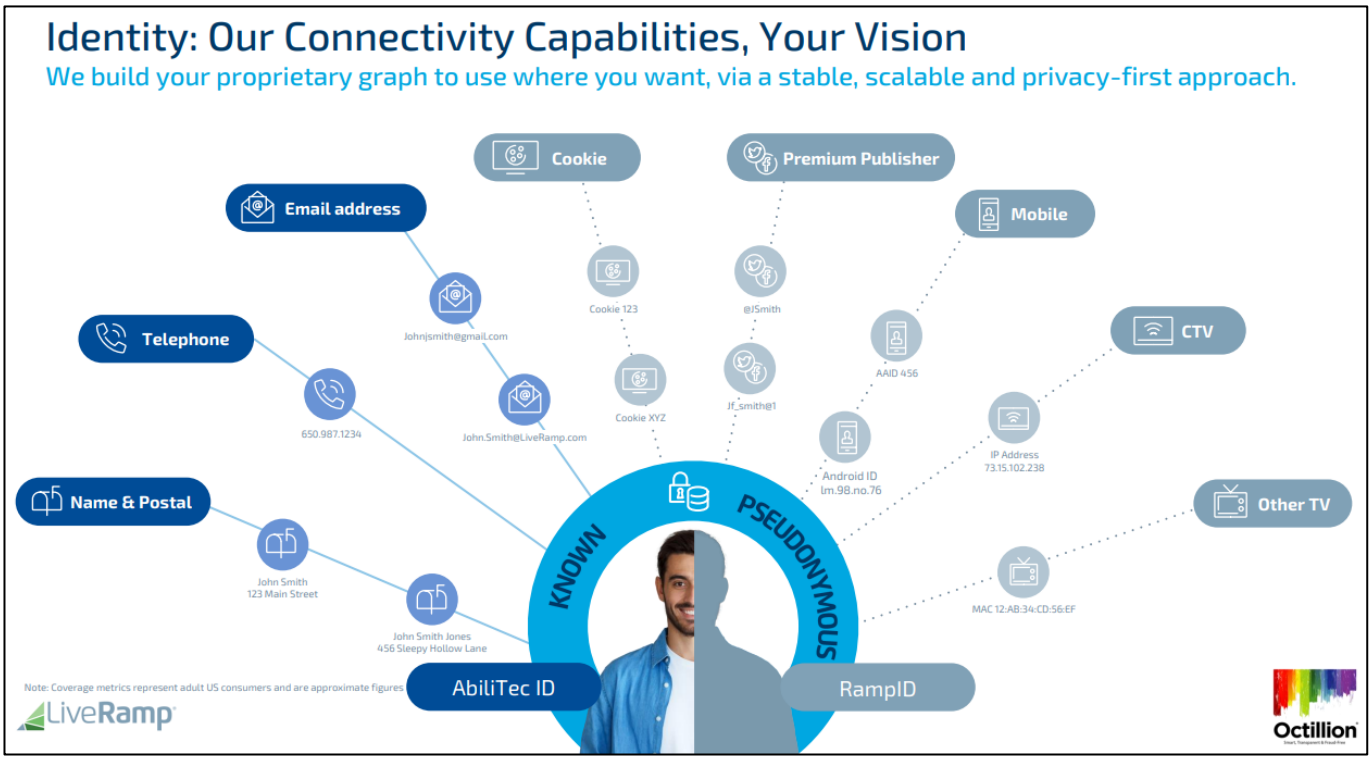


Figure 4 © LiveRamp

[89] https://developers.liveramp.com/rampid-api/docs/rampids [6.9.2023]
[90] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[91] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]
[92] https://docs.liveramp.com/connect/en/rampid-methodology.html [6.9.2023]
[93] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[94] https://web.archive.org/web/20220429143920/https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [29.4.2022]
[95] https://web.archive.org/web/20220627075101/https://docs.liveramp.com/connect/en/onboarding-your-data.html [27.6.2022]
[96] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[97] Ibid.
[98] LiveRamp (2022): The Future of Addressability. Page 10: https://files.ctctusercontent.com/75d73837001/e8858146-a9f4-4518-9bc1-b355b98065f3.pdf?rdr=true [6.9.2023]

LiveRamp provides extensive documentation about its RampID system:

- Many pages in the "help" docs cover RampID, in particular the "Connect"[99] and "Identity" docs[100]
- Many pages in the "RampID API" docs[101]

"Identity resolution" is defined by LiveRamp as "the process of resolving your data to a specific individual. The process matches personal identifiers (such as a name, address, phone, and email) to digital identifiers (such as an IP address, cookie, or location). The match is made across multiple devices and channels".[102] LiveRamp boasts that it "maintains the largest and most accurate people-based identity graph on the market", which "match[es] disparate cookies, proprietary platform IDs, mobile devices, and anonymized offline PII touchpoints" to its "common, people-based ID", the "RampID".[103] It states that it has an "online footprint of 14 billion devices",[104] and as such, **data about 14 billion devices**. The term "device" probably refers to any browser, smartphone, tablet or other device for which it has IDs . A single person may use several browsers and devices.

"Connect" is LiveRamp's cloud-based software that enables its clients to "upload" personal data, "manage" it (analyze and combine it, create "segments" etc), obtain third-party data from LiveRamp's marketplace and then further "distribute" personal data to hundreds of other companies (for further profiling, ad targeting, personalization and other purposes).[105]

2.2.1 RampID basics

The RampID system works very similar as the AbiliTec system. It provides the following key functionality:

- Clients can send all kinds of identifiers to LiveRamp (input data)
- LiveRamp tries to find an existing record in its identity graphs and returns one or several RampIDs, which are pseudonymous identifiers referring to individuals or households.

Clients can send different types of personal identifiers to LiveRamp in order to receive RampIDs:

- Name, street address, zip, city, phone numbers and/or email addresses in plaintext[106] ("PII", same as AbiliTec)
- Email addresses hashed with MD5, SHA1 or SHA256; phone numbers hashed with SHA1; combinations of name+email, name+phone or name+zip hashed with SHA1 ("hashed PII")[107]
- Browser cookie IDs, mobile device IDs (Google AAID, Apple IDFA), connected TV IDs (CTV IDs), custom IDs (CIDs)[108]
    - "Custom IDs" (CIDs) are more powerful than their vague name suggests. According to LiveRamp, a custom ID is an "account-based user ID understood by LiveRamp", a "partner" ID, an identifier that is "assigned to users by a specific platform, such as Google or Facebook". LiveRamp "often uses these types of identifiers as a cross-reference between a LiveRamp partner's ID and LiveRamp's IDs"[109] (see also sections 2.2.4 and 3.1.1)

The above list also represents the types of personal identifiers LiveRamp collects and maintains in its AbiliTec and RampID identity graphs.

LiveRamp describes three basic uses cases for the RampID system:[110]

- **"Offline PII merging: Resolving separate emails, postal addresses, and phone numbers to a single individual"**,

[99] https://docs.liveramp.com/connect/index.html [11.9.2023]
[100] https://docs.liveramp.com/identity/index.html [11.9.2023]
[101] https://developers.liveramp.com/rampid-api/ [7.9.2023]
[102] https://developers.liveramp.com/rampid-api/docs/about-identity-resolution [6.9.2023]
[103] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]
[104] Ibid.
[105] https://docs.liveramp.com/connect/index.html [6.9.2023]
[106] https://developers.liveramp.com/rampid-api/reference/batch-request-calls-match [7.9.2023]
[107] https://developers.liveramp.com/rampid-api/reference/batch-request-calls-lookup [7.9.2023]
[108] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[109] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[110] https://docs.liveramp.com/connect/en/rampid-methodology.html [6.9.2023]

- i.e. recognizing that identifying attributes collected in different contexts like names, postal addresses, email addresses and phone numbers refer to a single particular person. This functionality is also what the AbiliTec system has long been providing.

- **"Online device linking: Matching disparate devices to people-based pseudonymous identifiers"**,
  - i.e. recognizing that IDs referring to browsers, mobile phones and other devices collected in different contexts refer to a single particular person. This enables the exchange of other personal data about this person linked to these IDs across contexts.
- **"Offline to online: Merging these offline and online identity spaces into a unified, privacy-conscious, people-based ID space"**,
  - i.e. utilizing both "offline" and "online" identity data to recognize a person in all life contexts, which enables the exchange of other personal data about the person across contexts.

LiveRamp explains that it "deterministically matches offline personally identifiable information" (i.e. names, postal addresses, email addresses and phone numbers) and "online devices" (i.e. browsers, smartphones etc) to "people-based IDs". In addition, it "uses PII" (i.e. names, postal addresses, email addresses and phone numbers) to "deterministically link devices" (i.e. browsers, smartphones etc).[111] These three use cases are also reflected in sections 2.3 and 2.4 about identity graph data and identity graph data sources.

2.2.2 Maintained/derived/placeholder and household RampIDs

After receiving input data from clients as described in the previous section, LiveRamp returns three types of RampIDs referring to individuals:

- A **"maintained" RampID** "represent[s] an individual that LiveRamp fully recognizes".[112] A maintained RampID is returned when LiveRamp has a "persistent match for the input data",[113] when "there is a maintained record in the AbiliTec Identity Graph for the input data provided"[114], when LiveRamp has "a full understanding" of a "cookie or mobile device ID as an individual tied to multiple PII touchpoints".[115] Multiple browsers and devices may be linked to a single maintained RampID.[116]
- A **"derived" RampID** "represent[s] a PII touchpoint that LiveRamp is yet to match to a complete set of PII".[117] It is "associated with known PII (such as an email address or phone number)" but there is "no maintained record in the AbiliTec Identity Graph" for "the provided input data".[118] A derived RampID is returned when LiveRamp does "not have a persistent match for the input data"[119], when "a maintained RampID does not exist in our graph for the given device" and "LiveRamp has associated PII with this cookie or mobile device ID, but it is not complete".[120]
- A **"placeholder" RampID** "can be returned when no maintained or derived RampID exists" for a "given device"[121] such as a browser or a mobile device, for a "cookie or mobile device ID which LiveRamp has not identified".[122] It allows clients "to track online events even when the cookie or mobile device ID is not associated with PII".[123]

The following graphic from the docs also explains the differences between placeholder, derived and maintained RampIDs:[124]

[111] Ibid.
[112] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]
[113] https://developers.liveramp.com/rampid-api/docs/rampids [7.9.2023]
[114] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[115] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[116] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]
[117] Ibid.
[118] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[119] https://developers.liveramp.com/rampid-api/docs/rampids [7.9.2023]
[120] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[121] Ibid.
[122] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[123] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[124] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]

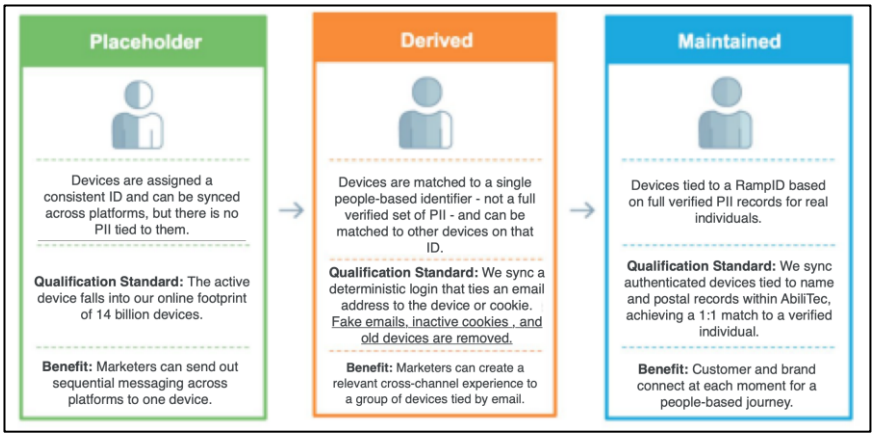


Figure 5 © LiveRamp

When LiveRamp receives a browser/cookie ID or mobile device ID but cannot link this ID to a person record in its identity graph, it returns a **placeholder RampID**. In this way, companies can still use a RampID to recognize the browser or device again at a later point in time and exchange other personal data about the user despite the absence of a full AbiliTec/RampID record. When LiveRamp is able to tie a cookie or device ID to at least one "PII" attribute such as an email address, but still cannot tie it to a full person record with multiple "PII" attributes in its identity graph, it returns a **derived RampID**. As soon as LiveRamp is able to tie the browser or device ID to a full person record stored in the AbiliTec system (a "verified" or "real individual", "tied to name and postal records within AbiliTec"[125]), it returns a **maintained RampID**.

Household RampIDs. In addition, LiveRamp can also return household RampIDs that are "tied to 1 or several maintained RampIDs".[126] A household RampID "represents adults living together at the same location who exhibit a persistent relationship. It is a pseudonymized version of an AbiliTec Household ID which is based on PII".[127]

Taken together, this suggests that LiveRamp maintains full "verified" person records that tie name, postal address, email addresses and phone numbers to one or many browser/cookie IDs and device IDs referring to the person. In addition, the system processes data about names, postal addresses, email addresses, phone numbers, browser/cookie IDs and device IDs that are somehow linked to each other, but do not refer to a full "verified" person record. It also processes data about single identifiers that are not linked to any other identifier and data about links between maintained records ("households"). This shows that LiveRamp collects and stores its identity graph data in different database tables or different databases and uses sophisticated methods to link all the identity records to each other. While this represents a technical measure that may improve data security, the system still enables far-reaching identity surveillance that helps many companies recognize persons across contexts and combine other personal data about them across contexts.

2.2.3 RampID formats, vendor-specific "encoding"

RampIDs are alphanumeric strings with either 49 or 70 characters, for example: [128] [129]

Maintained RampID (starts with "XY")	XY1234wXyWPB1SgpMUKIpzA0I3UaLEz-2lg0wFAr1PWK7FMhs
Derived RampID (starts with "Xi")	Xi1234p_iYcKP7ZlvFwwK9EwR8GKl_VJqIWUhEaAFmHLAjNOQ9b6OQzSkA43XiVFcTYQ9X
Placeholder/browser RampID ("Xc")	Xc1234p_iYcKP7ZlvFwwK9EwR8GKl_VJqIWUhEaAFmHLAjNOQ9b6OQzSkA43XiVFcTYQ9X
Placeholder/mobile RampID ("Xm")	Xm1234p_iYcKP7ZlvFwwK9EwR8GKl_VJqIWUhEaAFmHLAjNOQ9b6OQzSkA43XiVFcTYQ9X
Household RampID (starts with "hY")	hY1234wXyWPB1SgpMUKIpzA0I3UaLEz-2lg0wFAr1PWK7FMhs

Figure 6

[125] According to Figure 5
[126] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]
[127] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[128] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[129] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]

RampIDs are vendor-specific. Every RampID is specifically "encoded" for a certain client or partner. A RampID tied to a certain person, device or household looks different for every vendor, client or partner. Nevertheless, LiveRamp provides an API to convert RampIDs specific to one vendor to a RampID specific to another vendor ("transcoding"). This is another technical security measure that makes it difficult or impossible to "understand" or use RampIDs across companies without utilizing LiveRamp's "transcoding" service. As shown below, the "partner encoding" consists of four characters/bytes.[130] [131]

Figure 7 © LiveRamp

As section 3.2.1 shows, vendor-specific RampIDs are used by companies in the data industry which process data "on behalf" of thousands of their own clients and partners, including adtech firms and other intermediaries. While the fact that RampIDs are vendor-specific represents a technical measure that may improve data security, it does not generally prevent RampIDs from being used to link personal data across many actors in the industry. This is further addressed in section 3.2.

2.2.4 "Custom IDs" (CIDs), connected TV IDs (CTV IDs) and cookie IDs

This section provides additional information about LiveRamp's use of "custom IDs", connected TV IDs and cookie IDs.

Custom IDs (CIDs). In addition to names, postal addresses, phone numbers, email addresses, browser cookie IDs, mobile device IDs and connected TV IDs, LiveRamp's docs often mention "Custom IDs" (CIDs). According to LiveRamp, a custom ID is an "account-based user ID understood by LiveRamp", a "partner" ID, an identifier that is "assigned to users by a specific platform, such as Google or Facebook".[132]

- LiveRamp explains to consumers that CIDs "represent your identity to various partners we work with". They are "typically persistent and assigned to you when you create an account with our partners, e.g. a social media network, subscription service, or rewards program for retailers".[133]
- Facebook CIDs. A page in the LiveRamp docs states that "on a quarterly basis, LiveRamp sends Facebook a mapping file of pre-approved-for-marketing hashed PII tied to our Facebook CIDs (also referred to as "ExternIDs" by Facebook)". LiveRamp can find "Facebook CIDs that are tied to the same RampID". It can deliver "those matched CIDs" to Facebook, which "uses a mapping file it has generated in its backend to look up the CIDs it received and matches them to their Facebook IDs".[134] This suggests that LiveRamp links RampIDs to "Facebook CIDs", which are linked to Facebook users.[135]
- According to the docs, LiveRamp also uses CIDs to link data to Pandora and Pinterest users.[136]
- Third-party data providers can send CIDs as identifiers to LiveRamp.[137] In turn, LiveRamp can send CIDs as identifiers to "destinations" when LiveRamp's clients buy "segments" on LiveRamp's data marketplace.[138]
- At one point, LiveRamp mentions that it categorizes "TV device IDs" also as CIDs.[139]
- In a document filed filed to the California Privacy Protection Agency, LiveRamp explains that custom IDs "represent" a person's "identity to various partners" LiveRamp "work[s] with". They are "typically persistent and assigned to" persons

[130] https://developers.liveramp.com/rampid-api/reference/transcode-rampids-1 [7.9.2023]
[131] https://developers.liveramp.com/rampid-api/docs/rampid-transcoding-endpoint [7.9.2023]
[132] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[133] https://cppa.ca.gov/regulations/pdf/liveramp_sar_info.pdf [7.9.2023]
[134] https://docs.liveramp.com/connect/en/facebook-destination-account-integration-options.html [7.9.2023]
[135] See also section 3.1.1.3
[136] https://docs.liveramp.com/safe-haven/en/request-a-reach-estimate.html [7.9.2023]
[137] https://docs.liveramp.com/connect/en/transaction-signal-program.html [7.9.2023]
[138] https://docs.liveramp.com/connect/en/view-the-status-of-data-marketplace-segments.html [7.9.2023]
[139] https://docs.liveramp.com/advanced-tv/en/guide-to-creating-ip-address-based-files-for-upload.html [7.9.2023]

when they “create an account” with LiveRamp’s “partners, e.g. a social media network, subscription service, or rewards program for retailers”.[140]

CIDs appear to be personal identifiers assigned to persons by a larger number of LiveRamp’s partners, from platforms to large publishers to data brokers. They are another powerful component of LiveRamp’s identity graph. LiveRamp states that it “often uses” CIDs as a “cross-reference between a LiveRamp partner's ID and LiveRamp's IDs”.[141] LiveRamp may maintain database tables that map RampIDs to custom IDs from a larger number of third-party companies. It is not clear, however, which of these mappings are used in Europe.

When LiveRamp discusses sending input data for its RampID system, it “can accept cookies and custom IDs as input from any platform to which it can distribute data”[142] (see section 3.1.1 on what “distributing data” means). This suggests that LiveRamp’s clients and data partners can send either cookie IDs or custom IDs in order to retrieve RampIDs and map the sent personal data to LiveRamp’s identity graph. It also suggests that cookie IDs and custom IDs play a similar role. In some cases, LiveRamp may use cookie IDs to link personal records across companies. In other cases, it may use CIDs. Perhaps it sometimes uses both cookie IDs and CIDs.

LiveRamp sometimes also uses the term “Client Customer ID” (CCID), which appears to refer to internal customer IDs in client customer databases that remain in the scope of a single client.[143]

Connected TV IDs (CTV IDs). To recognize and link “smart” TV devices, LiveRamp uses the “TV Device ID (IFA)”, which it describes as “persistent TV device ID tied to the physical device”. LiveRamp emphasizes that a “TV device ID is also categorized” as a “Custom ID” or "CID". LiveRamp also collects IP addresses and device information (user agent) for TV devices. The “device type” attribute can have the following values: “rida” (Roku), “tifa” (Samsung), “lg” (LG), “chtv” (Chromecast), “atv” (Apple TV ID), “google_advertising_id” (Google), “idfa” (Apple), “windows_advertising_id” (Microsoft) and “amazon_advertising_id” (Amazon). The documentation states that LiveRamp will “filter” Apple TV IDs “out”. The documentation does not disclose whether this functionality is available in Europe.[144]

Cookie IDs. As detailed in section 2.4.2, LiveRamp synchronizes cookie IDs with third-party companies such as Google, Microsoft, Neustar, The Trade Desk and Quantcast. LiveRamp’s ID syncing practices based on third-party cookies rely on the ongoing exchange of cookie IDs with third-party companies. As such, these practices rely on the exchange of extensive personal data between LiveRamp and third-party companies. When LiveRamp discusses cookie IDs, it does not necessarily only refer to its “own” cookie IDs, but also to cookie IDs maintained by third-party companies, which it refers to as “partner cookie IDs”. To synchronize cookie IDs with a third-party company or “cookie syncing partner”, either LiveRamp or the third-party company (or both) must maintain a database that maps LiveRamp’s cookie IDs to the third-party company’s partner cookie IDs. The fact that LiveRamp was observed receiving partner cookie IDs from third parties suggests that LiveRamp operates such databases.[145]

Section 2.2.5.5 describes that LiveRamp can return maintained, derived or placeholder RampIDs based on providing it with cookie IDs. It is, however, not clear whether LiveRamp links partner cookie IDs directly to RampIDs in its identity graph. Perhaps partner cookie IDs are linked to LiveRamp’s own cookie IDs, which in turn are linked to RampIDs.

2.2.5 How to query and utilize the RampID system

LiveRamp clients can send data and receive RampIDs in very different ways. The following sections describe some query mechanisms, which provides further information about personal data flows in the context of the RampID identity graph.

[140] https://cppa.ca.gov/regulations/pdf/liveramp_sar_info.pdf [11.9.2023]
[141] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]
[142] Ibid.
[143] https://docs.liveramp.com/connect/en/onboarding-terms-and-concepts.html [7.9.2023]
[144] https://docs.liveramp.com/advanced-tv/en/guide-to-creating-ip-address-based-files-for-upload.html [7.9.2023]
[145] See section 2.4.2

2.2.5.1 Upload files with identifiers and receive files with RampIDs

By using LiveRamp's so-called "File-based Recognition Workflow (FBR), companies can upload files with identifiers and other data and receive files where the uploaded identifiers are replaced with RampIDs.[146] A client can, for example, upload a file that contains email addresses, gender and age (on the left) and receive a file that contains RampIDs rather than email addresses (on the right):[147]

Row	Email	Gender	Age
1	jane@doe.com	F	25
2	john@smith.com	M	45
3	jade@noe.com	F	56

Row	RampIDs	Gender	Age
1	RampID A	F	25
2	RampID B	M	45
3	RampID C	F	56

Figure 8 © LiveRamp

As this example shows, the files uploaded by clients can contain not only identifiers but also other personal attributes. The uploaded files can contain many columns with multiple identifiers and other personal attributes. Clients can use SFTP or Amazon/Google/Microsoft cloud storage to upload and receive files[148] in CSV and other formats.[149]

Types of identifiers to be uploaded. Clients can upload files to LiveRamp that contain names (first name, last name), postal addresses (street, city, zip), phone numbers, email addresses, cookie IDs, mobile device IDs (Apple IDFA, Google AAID) and custom IDs (CIDs). Some of those identifiers can optionally be uploaded in hashed format.[150]

LiveRamp states that "EU data files cannot contain hashed phone numbers. Email addresses are the only identifiers that can be hashed in EU data files".[151] It appears that phone numbers can still be uploaded in the EU, but not in hashed format. LiveRamp has a specific page about the creation of data files for "EMEA countries" in the docs that contains a list of "offline" identifiers that can be uploaded in the UK, France and Germany:[152]

- First name, last name, street address, town, postcode
- Up to three email addresses per uploaded record, either in plain text or hashed with MD5, SHA1 or SHA 256
- Up to three phone numbers

This represents, at the same time, evidence about the identifying attributes that LiveRamp collects and maintains in the EU. The page states that "only files containing offline identifiers are allowed".[153] This suggests that clients in the UK, France and Germany cannot upload "online" identifiers such as cookie IDs and mobile device IDs.

Some more EU, UK and FR specifics. LiveRamp states that clients must upload separate files per country that contain either "FR", "UK" or "DE" in the file name in a certain way .[154]

UK data files can contain a maximum of 100 million rows/records. FR data files can contain a maximum of 30 million rows/records. This illustrates the potential scale of personal data processing. LiveRamp restricts how often clients can upload "PII-based" data. For "UK data" there is a "maximum average of 1 file upload per day", for "French data" the limit is "1 file per week".[155]

---

[146] https://docs.liveramp.com/connect/en/file-based-recognition-workflow.html [7.9.2023]
[147] Ibid.
[148] https://docs.liveramp.com/connect/en/set-up-liveramp-file-deliveries.html [7.9.2023]
[149] https://docs.liveramp.com/connect/en/creating-data-files-for-emea-countries.htmlhttps://docs.liveramp.com/connect/en/creating-eu-data-files.html [13.9.2023]
[150] https://docs.liveramp.com/connect/en/formatting-identifiers.html [7.9.2023]
[151] Ibid.
[152] https://docs.liveramp.com/connect/en/creating-data-files-for-emea-countries.html [13.9.2023]
[153] Ibid.
[154] Ibid.
[155] Ibid.

AbiliTec/RampID upload and recognition process. When clients upload raw "PII" data to the RampID system, LiveRamp tries to match it to the "offline data in the AbiliTec Identity Graph". If a record is found, the uploaded data is linked to an AbiliTec ID. Finally, the AbiliTec ID is converted "into a pseudonymous, universal identifier called a RampID".[156]

Some more details on the process, including on security measures. Clients can optionally encrypt the files before sending it to LiveRamp, where they get decrypted. LiveRamp explains to use a sophisticated setup including two firewalls. The uploaded data is processed in a separate server environment. In the EU, the uploaded files are retained for 7 days. Matching and linking the data to an AbiliTec ID occurs in the "translation zone", an "essential component" of LiveRamp's identity services. Within this "translation zone", the uploaded "PII" data is "briefly" "loaded into memory" in order "to be replaced with a 16-character AbiliTec Link, which is then salted and hashed twice, converting it to a RampID (our pseudonymous identifier)". RampIDs can then be "translated" into vendor-specific cookie IDs, mobile device IDs and other digital identifiers in order to "distribute" data to "destinations", i.e. to link it to personal data processed by many other companies and platforms.[157]

LiveRamp does not return the rows in the same order as they have been sent. Optionally, it adds a "grouping indicator" that enables clients or, for example, "measurement partners", to "tie together all the RampIDs associated with each input record".[158] Generally, LiveRamp recommends to "use the RampIDs column" in order to tie disparate datasets together".[159]

2.2.5.2 Real-time access to the identity graph via the "RampID API"

LiveRamp's clients can use the "RampID API",[160] a "real-time interface that provides direct access to LiveRamp's Identity Graph".[161] The API provides four "endpoints" that provide different functionality:

- **"Match"** endpoint. Clients can send raw/plaintext names, postal addresses, phone numbers and/or email addresses[162] and receive up to 10 maintained or derived RampIDs that correspond to the input data. The input data goes through normalization, a "fuzzy matching" mechanism and the "match cascade". The first returned RampID is the best "match",[163] similar to the AbiliTec "Match" function (see section 2.1.4). If LiveRamp doesn't find a maintained RampID, it tries to return a derived RampID.[164] For each returned RampID, LiveRamp can include:
  - Match metadata (which attributes contributed to the match, confidence, name integrity etc)[165]
  - Information about whether the postal address, phone number or email address sent are the "best contacts" for the recognized individual (if address, phone or email were included in the input data)[166]
  - Information about whether the email address sent to the API is in active use, including the exact date and time the person clicked a link in an email received at this address as tracked by LiveRamp and its partners (if an email address was included in the input data)[167]
- **"Lookup"** endpoint. While the Match function allows to send plaintext identifiers and can be used to get extensive information about the input data sent to LiveRamp, the Lookup function tries to return a single maintained or derived RampID based on limited input data, for example based on sending a single email address.[168] Clients can send a hashed email address, a hashed phone number or a hashed combination of "name + email", "name+phone" or "name + zip" to LiveRamp.[169]
- **"Transcoding"** endpoint. Clients can convert RampIDs specifically "encoded" for one company or partner to RampIDs encoded for another company or partner.[170] For this purpose, companies send RampIDs encoded for one company to

---

[156] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]
[157] https://docs.liveramp.com/connect/en/liveramp-data-security-overview.html [6.9.2023]
[158] https://docs.liveramp.com/connect/en/file-output-options-for-file-based-recognition-workflows.html [7.9.2023]
[159] Ibid.
[160] https://developers.liveramp.com/rampid-api/ [7.9.2023]
[161] https://developers.liveramp.com/rampid-api/docs/the-basics [7.9.2023]
[162] https://developers.liveramp.com/rampid-api/reference/batch-request-calls-match [7.9.2023]
[163] https://developers.liveramp.com/rampid-api/docs/the-match-endpoint-1 [7.9.2023]
[164] Ibid.
[165] https://developers.liveramp.com/rampid-api/docs/matchmetadata-bundle [7.9.2023]
[166] https://developers.liveramp.com/rampid-api/docs/contactflags-bundle [7.9.2023]
[167] https://developers.liveramp.com/rampid-api/docs/emailinsights-bundle [7.9.2023]
[168] https://developers.liveramp.com/rampid-api/docs/the-lookup-endpoint-1 [7.9.2023]
[169] https://developers.liveramp.com/rampid-api/reference/batch-request-calls-lookup [7.9.2023]
[170] https://developers.liveramp.com/rampid-api/docs/rampid-transcoding-endpoint [7.9.2023]

LiveRamp and receive RampIDs referring to the same individuals encoded for another company. LiveRamp states that it validates "certain privacy restrictions" before granting a company access to the ability to transcode RampIDs and requires a confirmation from both companies who want to transcode (i.e. exchange) RampIDs. It appears that the involved companies grant the permission to transcode RampIDs via email.[171] Section 3.2.1 provides more information on "transcoding".

- **"Identity Envelope Decryption"** endpoint**.** Clients can use the RampID API to decrypt "identity envelopes", which are encrypted versions of RampIDs that look different even for the same underlying data every time they are created. Only LiveRamp knows which RampID (=person) an "identity envelope" refers to.[172] "Identity envelopes" are a key component of LiveRamp products that rely on RampIDs such as ATS (see section 3.3).

The RampID API docs rarely provide any information about whether or how the API can be used in the EU. LiveRamp's UK website promotes the "Retrieval API",[173] which was renamed "RampID API" in 2022.[174] LiveRamp may also maintain internal APIs that are not directly provided to clients or only to certain clients and offer more extensive functionality.

2.2.5.3 "Onboarding" data to LiveRamp „Connect"

Clients can upload records with identifying data to LiveRamp's cloud-based "Connect" platform, which tries to recognize the corresponding persons using the RampID system. LiveRamp and other data companies call this process "onboarding".[175] Clients can then make extensive use of the "onboarded" personal data, analyze it, combine it with other personal data, and then use it across the digital world by "distributing" it to hundreds of "destinations", for example, to other data, adtech and marketing intermediaries, platforms and publishers.[176]

"Onboarding" steps:[177]

- Clients upload files that contain records with identifying information and other personal data, similar to what was described in section 2.2.5.1
- RampID recognition. LiveRamp tries to match the uploaded records to person records in its identity graph by first creating AbiliTec IDs and then RampIDs.
- Segmentation. The personal attributes which are uploaded in addition to identifiers are organized into "fields" and "segments" (see below).
- "Distribution". Fields and segments are being sent to one out of several hundred of LiveRamp's partners, which LiveRamp refers to as "destinations".
- "Activation". To distribute data to destinations LiveRamp sends RampIDs, cookie IDs, mobile device IDs or other digital IDs to them so they can recognize or address the person the distributed data is about.
- "Delivery". LiveRamp delivers the "activated" data that should be distributed to the "destinations".

The uploaded files must contain a column for every row that LiveRamp can use as an "audience key", which must be unique for every row. This can be a client customer ID (CCID) or another type of identifier.[178]

Example of an "onboarding" data file uploaded to LiveRamp:[179]

```
CCID,FIRSTNAME,LASTNAME,ADDRESS1,ADDRESS2,CITY,STATE,ZIP,EMAIL1,SHOPPERSCORE,LOVESDOGS,UNDER25,FAVORITECOLOR,PREVIOUSCITY
35938495,Jane,Doe,100 Main St,Apt. A,Anytown,CA,123454545,jane.doe@email.com,54,1,1,Green,"San Francisco, CA"
103578302,John,Dough,123 Any St,,Anytown,CA,123456565,john.dough@email.com,87,1,,Blue,"Bend, OR"
902833740,Sam,Sample,555 New Rd,Fl 17,Mysteryville,OK,957352436,sam.sample@email.com,36,,1,Red,"Ames, IA"
328697301,Sarah,Sampel,987 Imaginary Ln,,Buffetown,MI,436237235,sarah.sampel@email.com,99,,,Blue,"Rochester, NY"
993802274,Dolly,Data,456 Center Ave,,Newtown,NE,586452778,dolly.data@email.com,12,1,,Yellow,"Athens, GA"
```

Figure 9 © LiveRamp

[171] https://developers.liveramp.com/rampid-api/docs/rampid-transcoding-endpoint
[172] https://developers.liveramp.com/rampid-api/docs/envelope-decryption-endpoint [7.9.2023]
[173] https://liveramp.uk/developers/product/identity/ [7.9.2023]
[174] https://web.archive.org/web/20220626071910/https://developers.liveramp.com/retrieval-api
[175] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]
[176] https://partner-directory.liveramp.com/ [7.9.2023]
[177] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]
[178] Ibid.
[179] https://docs.liveramp.com/connect/en/formatting-column-based-files.html [7.9.2023]

The above example file could, for example, represent an excerpt of a customer database from a company that wants to "onboard" its customer data via LiveRamp "Connect". The CCID column represents the internal customer number. Each row contains identifying information (first name, last name, address, city, state, zip, email) and other personal attributes, in this case a "shopper score", the favorite color of the person, the city where the person previously has been living, and information about whether the person "loves dogs" and is under 25 years old or not. It represents a basic customer profile.

LiveRamp uses several concepts that describe how it organizes the uploaded personal attributes in its "Connect" system:[180]

- **Fields and values.** A field is a personal attribute or category that can have different values.[181] In the above example file, the field "Loves Dogs" can contain the value "1" (or it can be empty). The field "Previous City" can contain "San Francisco, CA", "Bend, OR" and other values. The field "Favorite color" can contain the values "Green", "Blue", "Red" and "Yellow". With the help of fields, the uploaded records turn into digital profiles of persons stored in the "Connect" system. LiveRamp provides different types of fields, e.g. "enumerated fields" with less than 250 distinct values, "raw fields" with more than 250 distinct values, "binary" fields, "numeric" fields, "string" fields etc.[182]
- **Segments.** A segment is a group of records about persons where a field has the same value. In the above example, the segment "Favorite color = Blue" would contain 2 records (the second and the fourth one). Other segments could, for example, contain records where the value of the field "shopper score" is above a certain number. As LiveRamp matches each row uploaded to its system to RampIDs, a segment is actually a list of IDs referring to persons with certain characteristics.
- **Audience.** In LiveRamp's "Connect" system, the term "audience" refers to a set of uploaded files, segments, fields and values (other data and adtech companies often use the term "audience" synonymous to "segment").

The graphic below, extracted from LiveRamp's docs[183], shows a hypothetical retail company that uploaded four files to LiveRamp, each containing more than 250,000 records. The uploaded files include the company's entire customer database ("1st Party CRM Database"), store transaction data ("In-Store Transaction Data") and a data set purchased from a third party firm ("3rd Party Acquisition List"). This illustrates the possible scale of these personal data processing activities.

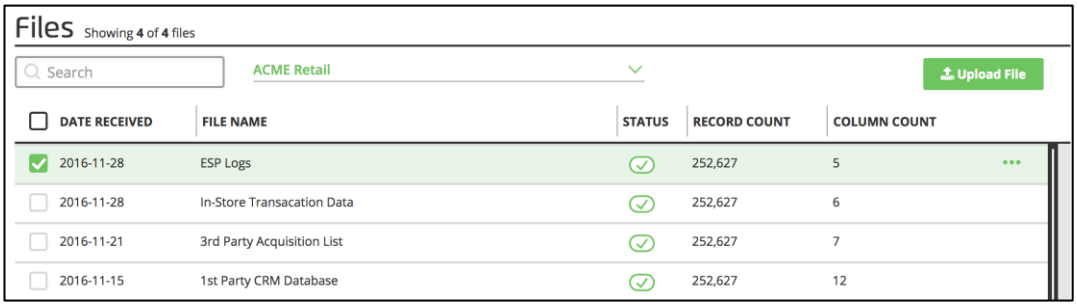


Figure 10 © LiveRamp

After "onboarding" personal data via "Connect", clients can further send the data to many other companies for several different purposes (see section 3.1.1). Both "onboarding" data and sending it to "destinations" relies on LiveRamp's identity graph systems. LiveRamp also allows "resellers" to resell LiveRamp's "onboarding" services.[184] It is not clear how many resellers do so and whether large companies are among them.

2.2.5.4 LiveRamp's tracking tags for the web and mobile apps

LiveRamp provides different "tags" that can be embedded into client websites or "attached" to digital ads. They illustrate some powerful and intrusive types of applications of LiveRamp's RampID system:

---

[180] https://docs.liveramp.com/connect/en/onboarding-terms-and-concepts.html [7.9.2023]
[181] Ibid.
[182] https://docs.liveramp.com/connect/en/types-of-segment-data-fields.html [7.9.2023]
[183] The graphic was accessible until April 2022: https://web.archive.org/web/20220429143907/https://docs.liveramp.com/connect/en/match-reports.html
[184] https://docs.liveramp.com/connect/en/reseller-onboarding.html [7.9.2023]

- **"Real-Time Identity Service Tag" (RTIS)[185] for the web.** Websites that implement LiveRamp's RTIS tag receive a RampID corresponding to the website visitor, whether the user is logged in or an "anonymous" visitor. They can then use the RampID, for example, for "personalization and measurement", i.e. to profile users and make decisions about them. They can "leverage offline and third-party data to make more informed decisions for that user" because "offline and third-party data can be matched to the same people-based RampIDs". Clients can also "attach" the RTIS tag to digital ads displayed somewhere on the web, and then track users who interact with the ad. LiveRamp mentions that the tag is "certified to run on a number of platforms, including Google AdX". By "resolving website and ad impressions to people in real-time," clients "can access people-based data immediately at the time of impression".
    - The RTIS tag appears to make extensive use of LiveRamp's cookie ID tracking in order to recognize website visitors and attach RampIDs to them. LiveRamp explains that by "leveraging LiveRamp cookies, the Real-Time Identity Service gives you direct access to the large scale of LiveRamp recognition, regardless of whether or not you have the user synced with LiveRamp or even if you have cookied the user".
    - The RTIS tag sends HTTP requests to LiveRamp that look like: https://id.rlcdn.com/<TAG ID>.gif
    - LiveRamp states that it "might" require "special paperwork" from clients who use the RTIS tag in the EU.
- **Client-Side Tag (CST)[186] for the web and mobile apps.** Websites can implement LiveRamp's CST tag to send data on user activities such as "page views", "ad views", "adding items to a cart" or "completing a transaction" to LiveRamp. Clients can then use the LiveRamp "Connect" platform to create segments and make further use of the data. For example, they could create and constantly update a segment that contains all users that have started registering on the website. The captured data goes through LiveRamp's recognition process including matching website visitors to RampIDs. The CST tag automatically "captures" the URL of the web page visited and the exact date and time of the visit and can capture additional information, which is customizable. In addition to using the data in the "Connect" system, clients can receive log files that contain data on all the captured interactions including RampIDs. CST tags can not only be be placed on websites, but also "in advertisements to capture ad impressions".
    - While the standard CST tag is embedded in websites and utilizes LiveRamp's cookie IDs to recognize website users, the "Enhanced Client-Side Tag" (eCST) can also be placed in mobile apps or apps for connected TVs. The eCST tag can also capture "mobile device IDs, OTT IDs and CTV IDs" and use them to recognize persons via the RampID system. In addition, the eCST tag can also capture "identity envelopes" generated by LiveRamp's ATS product and use them to recognize users and push the data to "Connect".[187]
    - The CST/eCST tag sends HTTP requests to LiveRamp that look like:
      https://di.rlcdn.com/api/segment?pid=<TAG ID>
- **Real-Time CID Delivery Tag[188] for the web.** The CID tag enables websites to recognize "anonymous" website visitors not by receiving RampIDs but by receiving their "own" Custom IDs (CIDs), i.e. identifiers assigned to persons by platforms, publishers and data brokers (see section 2.2.4). To make this work, clients and platforms must regularly upload files to LiveRamp that map their CIDs to personal identifiers such as names, postal addresses, email addresses and phone numbers.
    - The tag's HTTP requests to LiveRamp look like: https://so.rlcdn.com/<TAG ID>.gif

LiveRamp provides additional "tags" that are not related to its clients' use of the RampID system, but to the contribution of data to LiveRamp's identity graph data, the synchronization of cookie IDs with LiveRamp's partners or the collection of links between cookie IDs and email addresses (see sections 2.4.2 and 2.4.3).

2.2.5.5 Receive "mapping files" that contain RampIDs and other identifiers

Several services offered by LiveRamp including the CST tag (see previous section) and other "Connect" services provide a mechanism that delivers so-called "mapping files" to clients "on a regular basis", which allows clients to "see a mapping between an external identifier (such as a cookie, mobile device ID, connected TV ID, or custom ID) and a RampID". These files

[185] https://docs.liveramp.com/identity/en/implementing-liveramp-s-real-time-identity-service-tag.html [7.9.2023]
[186] https://docs.liveramp.com/identity/en/implementing-liveramp-s-client-side-tag.html [7.9.2023], https://docs.liveramp.com/identity/en/implementation-methods-for-client-side-tags.html [7.9.2023], https://docs.liveramp.com/identity/en/data-automatically-captured-for-client-side-tags.html [7.9.2023], https://docs.liveramp.com/identity/en/placing-client-side-tags-in-advertisements.html [7.9.2023]
[187] https://docs.liveramp.com/identity/en/implement-the-enhanced-client-side-tag.html [15.9.2023]
[188] https://docs.liveramp.com/identity/en/implementing-liveramp-s-real-time-cid-delivery-tag.html [7.9.2023]

can also include the date and time the corresponding ID has been "seen" (processed) the last time. Clients can decide about how often they want to receive these files, whether they want to receive full files or incremental updates and which types of RampIDs they want to receive (maintained, derived, placeholder, household). Clients can use these files to "[power] targeting and measurement", "[recognize] non-logged in users" on a website for personalization and to "[improve] monetization", according to LiveRamp.[189] Here's how a mapping file with cookie IDs, individual RampIDs and household RampIDs can look like:[190]

Cookie_ID	RampID	HH_RampID	Last_seen_at
Cookie123	XY1234abc...	hY1234cfe...	1560194527000
Cookie456	XY1234cde...	hY1234clk...	1560099103000
Cookie789	XY1234dgt...	hY1234def...	1563497974000

Figure 11 © LiveRamp

LiveRamp states that a "cookie mapping file is generated by collecting site traffic". The client must "enable this by implementing a cookie sync with us through the use of a pixel". Mobile "device ID mapping files (for IDFA and AAID) are built from our mobile device mapping pool, which is powered by the site traffic from our entire match partner network".[191]

2.3 Identity graph data

The previous sections describe how LiveRamp's AbiliTec and RampID systems work and how they can be used by clients. This section summarizes the types of personal data LiveRamp collects and processes to provide its identity graph services, in part based on the findings from the previous sections. A recent annual report filed to the SEC suggests that LiveRamps's identity graph contains personal data about 700 million consumers globally (see section 2).

2.3.1 "Offline" information (AbiliTec data, "PII" data, names, addresses, email, phone)

LiveRamp describes its AbiliTec identity graph as "a vast, multi-sourced historical identity graph containing over 40 years of consumer contact information from over 150 data sources, including over 4.5 billion name and postal records, over 1.1 billion email addresses, and over 600 million phone numbers".[192] LiveRamp's UK and French websites stated in 2022 that it has data on 25 million people in France[193] and on 45 million people in the UK[194] based on "100+ sources for offline, historical information".[195] According to LiveRamp, its "offline data asset" is the "backbone" of its identity graph.[196]

According to the docs, LiveRamp knows about names, name variations, postal addresses, email addresses and phone numbers.[197] More specifically, it knows about data categories like first name, middle name, last name, street address, city and zip.[198] It may store and process more than one instance of attributes such as email addresses or phone numbers per person.[199] In addition, it stores "consumer associative data, such as gender or year of birth (used to build people and household formations)" and "Internal metadata, such as frequencies, classifications, and thresholds for making linking decisions".[200] Most important, it stores and processes personal data about the links and associations between identifying attributes, for example,

[189] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[190] Ibid.
[191] Ibid.
[192] https://developers.liveramp.com/AbiliTec-api/docs/the-AbiliTec-identity-graph-1 [5.9.2022]
[193] https://liveramp.fr/notre-plateforme/identity-graph/ [22.6.2022], https://web.archive.org/web/20220820055217/https://liveramp.fr/notre-plateforme/identity-graph/
[194] https://liveramp.uk/our-platform/identity-graph/ [22.6.2022], https://web.archive.org/web/20220613155152/https://liveramp.uk/our-platform/identity-graph/
[195] Ibid.
[196] Ibid.
[197] https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [5.9.2023]
[198] https://developers.liveramp.com/AbiliTec-api/reference/match-single-transaction-calls [5.9.2023]
[199] https://docs.liveramp.com/connect/en/creating-eu-data-files.html [7.9.2023]
[200] https://docs.liveramp.com/identity/en/understanding-AbiliTec.html [5.9.2023]

about which attributes refer to a person, how persons are linked to places and addresses and which persons belong to a household. It also stores information about "maintained" and "derived" identifiers.[201]

LiveRamp's UK and French services privacy policies discuss "offline" data a lot. Both state that LiveRamp collects names, birthdates, postal addresses, email addresses and phone numbers.[202] The UK policy describes that the company also collects personal attributes like "marital status, title, date of birth, and gender" and other "attributes (such as demographic data)".[203]

2.3.2 "Online" information (browser, device and "custom" IDs)

As detailed in section 2.2, the RampID system adds personal identifiers referring to browsers, devices and to digital profiles maintained by third-party companies to LiveRamp's identity graph. This includes cookie IDs maintained by LiveRamp and other companies, mobile device IDs (Apple IDFA, Google AAID), connected TV IDs (CTV IDs) and so-called custom IDs (CIDs).[204] As section 2.2.4 shows, this can also include IP addresses. Sections 2.2.4 and 2.4.2 provide further details about how LiveRamp collects and processes cookie IDs, custom IDs and connected TV IDs. LiveRamp states that it has an "online footprint of 14 billion devices",[205] and as such, "online" information about **14 billion devices**. The term "device" probably refers to any browser, smartphone, tablet or other device for which it has an ID. A single person may of course use several browsers and devices.

Once again, LiveRamp also stores and processes personal data about the links and associations between these personal identifiers. As detailed in section 2.2.2, "placeholder" RampIDs are linked to "online" identifiers such as single cookie IDs or device IDs. "Derived" or "maintained" RampIDs are linked to both "online" and "offline" identifiers.

LiveRamp's French services privacy policy states that the company also collects "associated data" such as "IP address, User Agent, timestamp, URL or app name, etc" in the context of its "recognition and synchronization solutions".[206] The UK services privacy policy states that the company collects "technical data" such as IP address, "log-in data, web browser type and version used, time zone setting and country, browser plug-in types and versions, operating system and platform, and other technology on the devices [people] use to access websites", but is less specific about the context and purpose of this data collection.[207] A document filed to the Californian privacy regulator indicates that LiveRamp collects "pixel serving log data", which includes the URL a "pixel was fired from", the user's IP address and information about device type, browser and operating system.[208]

2.3.3 Links between "online" and "offline" information

In addition, the RampID system stores and processes personal data about the links and associations between "offline" information (such as names, postal addresses, email addresses and phone numbers) and "online" information (such as cookie IDs, mobile device IDs, connected TV IDs and custom IDs). As detailed in section 2.2.2, a "derived" RampID is, for example, linked to an "online" identifier" such as a cookie ID or mobile device ID and an "offline" identifier such as an email address or a phone number. A "maintained" RampID is, for example, linked to multiple "online" and "offline" identifiers.

As section 2.4.3 details, LiveRamp obtains personal data about links between "online" and "offline" identifiers from its "match network", which consists of "match partners" who send or sell combinations of identifiers to LiveRamp. LiveRamp receives, for example, hashed email addresses and corresponding cookie IDs from websites when users register or log in. LiveRamp also receives hashed email addresses and corresponding device IDs from mobile apps. According to the company, it receives information about "**600 million unique online authentication events per month**" across its "match network".[209] As a result,

---

[201] See section 2.1

[202] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023], https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]

[203] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]

[204] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]

[205] Ibid.

[206] Original in French, direct quotes in English via Google Translate: https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]

[207] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]

[208] https://cppa.ca.gov/regulations/pdf/liveramp_sar_info.pdf [11.9.2023]

[209] https://liveramp.com/developers/blog/rampup20-for-developers-recap-architecture-and-future-liveramp-platform/ [11.9.2023]

LiveRamp maintains data about "45 million matched UK people"[210] and "25 million matched people"[211] in France, according to its UK and French websites.

2.3.4 How does LiveRamp store personal data internally?

It is not clear how LiveRamp actually stores personal data with respect to its identity graph in its internal systems. As the previous sections show, it uses a variety of technical measures to pseudonymize, hash and otherwise obfuscate personal identifiers. LiveRamp states, for instance, that its AbiliTec identity graph is "non-discoverable, meaning the data stored within it has been obfuscated and is not retrievable by any client, third party, or any LiveRamp associate who is not directly involved in its development or support. It is only used for analysis to create and maintain AbiliTec IDs".[212] A document filed to the California Privacy Protection Agency indicates that LiveRamp stores personal attributes such as names, postal addresses and email addresses in plaintext format in the US.[213] In any case, LiveRamp stores and processes a large amount of pseudonymous identifiers, which refer to persons and can be used to track, follow, profile and target them.

2.4 Identity graph data sources

LiveRamp obtains personal data for its AbiliTec and RampID identity graph systems from several sources.

When the company's clients send or upload personal data to LiveRamp to let it recognize people and utilize the resulting AbiliTec and RampID identifiers for different purposes, LiveRamp certainly does not always include all the client data in its identity graphs. Most likely, LiveRamp offers contracts to some clients that explicitly forbid LiveRamp to use client data for its own business purposes. In other cases, clients may have contracts that explicitly allow LiveRamp to include client data in its identity graphs. Sometimes, LiveRamp may incentivize clients to allow it to use client data for its own purposes by promising them better services or other benefits. This may differ between regions. In yet other cases, companies might just provide personal data to LiveRamp without using its other services. The next sections show that LiveRamp "purchases" identity data and tells companies that they can "monetize" and sell data to LiveRamp for its identity graph systems.

LiveRamp states that its identity graph is "composed of three linkage networks, the LiveRamp offline and online match networks, and LiveRamp's partner network of online integrations". This explanation is followed by the below chart:[214]

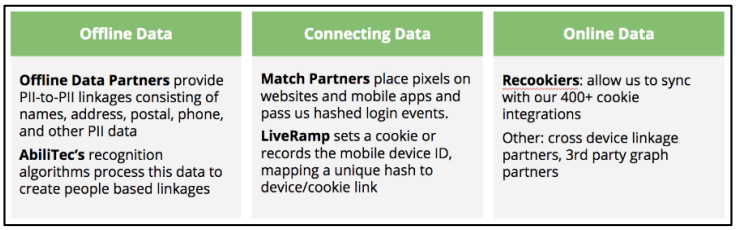


Figure 12 © LiveRamp

This chart and the information laid out in the next sections suggests that these "three linkage networks" refer to the following types of identity graph data sources:

- "Offline" "match networks" refer to "offline data partners" who provide "offline" information such as names, postal addresses, email addresses and phone numbers and links between these identifiers.
- "Online" "match networks" refer to browser/cookie syncing partners who help LiveRamp to establish a distributed personal identifier for people using the web browser.
- LiveRamp's "partner network of online integrations" refers to its "match partners" who provide links between "offline" identifiers such as email addresses and "online" identifiers such as cookie IDs and mobile device IDs.

---

[210] https://liveramp.uk/our-platform/identity-graph/ [22.6.2022], https://web.archive.org/web/20220613155152/https://liveramp.uk/our-platform/identity-graph/

[211] "Atteignant plus de 25 millions de personnes appariées en ligne": https://liveramp.fr/notre-plateforme/identity-graph/ [22.6.2022], https://web.archive.org/web/20220820055217/https://liveramp.fr/notre-plateforme/identity-graph/

[212] https://developers.liveramp.com/AbiliTec-api/docs/the-AbiliTec-identity-graph-1 [5.9.2022]

[213] https://cppa.ca.gov/regulations/pdf/liveramp_sar_info.pdf [11.9.2023]

[214] https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [10.9.2023]

The next sections describe these three types of data sources for LiveRamp's identity graph.

2.4.1 Sources for "offline" identifiers and links between them – LiveRamp's "offline" data providers

The AbiliTec identity graph is, according to LiveRamp, a "series of reference bases that are non-discoverable, multi-sourced data repositories". It relies on a "multi-billion record set of historical reference bases". It is "sourced from hundreds of contributors", contains "multiple name, address, and email representations for individuals, as well as the associative data to resolve the data points to an individual over time" and it is "continually updated and benchmark tested". Before "a new data source is added to the repository, LiveRamp carefully vets the source to ensure the compliance, quality, reliability, contribution value, and sustainability of the data". The "types of sources" include "public record data", "publically available data" and "self-reported information".[215] While the availability of "public records" and "publicly available data" differs in different regions and countries, "self-reported information" may actually refer to personal data obtained or purchased from other companies. LiveRamp typically does not have direct relationships with consumers.

LiveRamp states that "PII-to-PII linkages consisting of names, address, postal, phone and other PII data" are provided by "offline data partners".[216] It "purchases its email-to-postal address match data from various third-party providers".[217]

LiveRamp's UK services privacy policy explains that the company collects personal data from a "variety" of "data sources" it refers to as "offline database providers", which it uses "for identity matching and recognition carried out on behalf" of its clients. LiveRamp explains to consumers that these offline database providers "may have obtained your personal data because you provided it to them directly (such as by completing a lifestyle survey), because you bought goods from that company or its providers, or because you subscribed to services provided by that company or its own providers". More generally, "offline information" processed by LiveRamp "may also originate from third parties who may not have a direct relationship with you but collect offline information from their own offline sources".[218]

LiveRamp's French services privacy policy explains that it collects "directly identifying data" including "surnames, first names, dates of birth, postal addresses, email addresses and telephone numbers" through its "trusted partners" or "offline partners", who "obtain information declared voluntarily by individuals through questionnaires when purchasing goods or subscribing to a service, for example". Furthermore, LiveRamp states that it uses "information obtained from public sources such as INSEE or the register of companies and company directors". In addition, the French services privacy policy explains that readers could consult a "list of partners" including "offline partners" when following a link to the web page about LiveRamp's "partners".[219] As of 2023, this page does not contain information about "offline partners" anymore.[220] Until 2022, the page listed the following French "offline partners":[221]

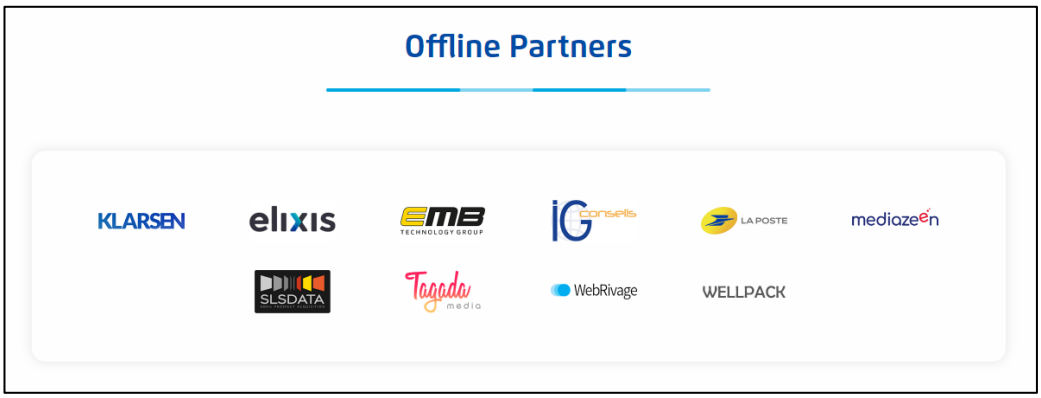


Figure 13 © LiveRamp

[215] https://docs.liveramp.com/connect/en/rampid-methodology.html [6.9.2023]
[216] https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [10.9.2023]
[217] https://docs.liveramp.com/connect/en/liveramp-match-data-sources.html [10.9.2023]
[218] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]
[219] Original in French, direct quotes in English via Google Translate: https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]
[220] https://liveramp.fr/partenaires/ [10.9.2023]
[221] https://web.archive.org/web/20220523082051/https://liveramp.fr/partenaires/

LiveRamp's **"Addressability Extension"**[222] program looks like a detailed documentation about how companies can contribute data to the identity graph. As a part of this program, LiveRamp asks clients to make "offline data contributions" while they make use of LiveRamp's identity and recognition services. When they take part in the program, LiveRamp "collects the linkages of two or more raw (unhashed) consumer PII touchpoints that you upload to LiveRamp in batch files and stores them in a secure internal environment. These linkages are added as additional PII touchpoints in our Identity Graph". LiveRamp promises that the "raw PII is never exposed" when they "match client data into the graph".[223] An extra page in the docs about how clients can contribute "offline data" via the "Addressability Extension" program explains that LiveRamp prefers to just use the files clients upload for "onboarding" purposes for its identity graph database as well, but clients can also send separate files to LiveRamp. In this case, clients should upload a "file containing all known PII touchpoints for the consumers in [their] CRM", i.e. clients should upload their entire customer database. Each uploaded record "must include two or more PII touchpoints for that record to be utilized". Examples of "PII touchpoints" to upload include "Name and Postal Address (First Name, Last Name, City, State, Street Address, and ZIP Code)", "Email Address" and "Phone Number".[224]

To contribute data via the "Addressability Extension" program, data providers must sign the "Addressability Extension terms", which may already be part of their "existing contract" with LiveRamp. LiveRamp also states that it will review the data providers "privacy policy" to "verify" that it "has adequate language and opt-out options, including specifying how you're using consumer data". If data providers are not "immediately approved", LiveRamp will provide them "with specific language that we would suggest you use so that you are compliant with our match policies".[225] It is not clear whether the "Addressability Extension" program really describes how LiveRamp obtains "offline" data in Europe today. It might be only a supplemental program and/or LiveRamp has custom contracts and agreements with "offline" data providers.

2.4.2 Sources of (and recipients for) cookie IDs – LiveRamp's browser/cookie syncing network

While third-party data companies such as LiveRamp can easily identify users of smartphones and other devices that provide unique device identifiers which refer to the users of these devices, it was never trivial for them to identify people visiting websites via the web browser. As web browsers do not provide unique identifiers which consistently refer to their users, third-party data companies started to exploit several web and browser features (cross-domain HTTP requests, third-party cookies and other browser storage technologies) to create personal identifiers for the users of browsers. These personal identifiers are referred to as **cookie IDs**. Many websites embed software from third party companies (e.g. "tags" and "pixels") that stores cookie IDs in the user's browser, which they can retrieve during subsequent visits to these websites. As such, third-party companies can recognize website visitors when they return to these websites at a later point in time.[226]

When third-party companies want to exchange personal data about the behaviors or characteristics of website visitors among each other, they must ensure to "talk" about the same users. For this purpose, they map cookie IDs maintained by one third-party company to cookie IDs maintained by another third-party company. This process, which involves the exchange of cookie IDs between these third-party companies, is often referred to as **cookie syncing** or **ID syncing**. As a result, third-party companies can persistently identify users of web browsers and thus recognize, track, follow, profile and target people across companies and websites.[227] In a nutshell, cookie/ID syncing uses distributed personal data processing at scale to create what

---

[222] https://docs.liveramp.com/connect/en/addressability-extension.html [10.9.2023]

[223] Ibid.

[224] https://docs.liveramp.com/connect/en/integrating-offline-data-into-addressability-extension.html [10.9.2023]

[225] https://docs.liveramp.com/connect/en/addressability-extension.html [10.9.2023]

[226] See e.g. Englehardt, Steven and Narayanan, Arvind (2016): Online Tracking: A 1-million-site Measurement and Analysis. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 1388–1401. DOI: https://doi.org/10.1145/2976749.2978313; Quan Chen, Panagiotis Ilia, Michalis Polychronakis, and Alexandros Kapravelos. 2021. Cookie Swap Party: Abusing First-Party Cookies for Web Tracking. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 2117–2129. DOI: https://doi.org/10.1145/3442381.3449837; Ido Sivan-Sevilla & Patrick T. Parham (2022): Toward (Greater) Consumer Surveillance in a 'Cookie-less' World: A Comparative Analysis of Current and Future Web Tracking Mechanisms. Online: https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Parham-Toward-Greater-Consumer-Surveillance-in-a-Cookie-less-World.pdf; from p. 79: Christl, Wolfie (2022): Digital Profiling in the Online Gambling Industry – Technical Report. Analysis of Personal Data Flows based on Subject Access Request information and Browser Tests. A report by Cracked Labs commissioned and published by Clean Up Gambling, January 2022. Online: https://crackedlabs.org/en/gambling-data; Christl, Wolfie und Sarah Spiekermann (2016): Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wien 2016. https://crackedlabs.org/en/networksofcontrol

[227] Ibid.

is not available in the web browser, a unique **personal identifier for the web browser**. While some browser vendors have restricted the use of third-party cookies for identification purposes in recent years, it still seems to be very prevalent in the dominant Chrome browser.[228]

As the cookie/ID syncing process involves the constant exchange of cookie IDs between these third-party companies, it involves the constant exchange of personal data across many companies at a massive scale. When LiveRamp synchronizes its "own" cookie IDs with cookie IDs maintained by other companies, it constantly receives personal identifiers from other companies and sends personal identifiers to other companies. A previous investigation of cookie/ID syncing practices by the author found that LiveRamp processed its "own" cookie IDs across visits to websites operated by different companies and received cookie IDs from two other data companies (Google, MediaMath).[229]

LiveRamp states that it synchronizes cookie IDs with "400+" third-party companies via its "400+ cookie integrations", [230] including with Google, Microsoft, Neustar, Nielsen, The Trade Desk and Quantcast.[231] LiveRamp's French website stated in 2022 that its "sync partners" include Facebook, Google, Amazon, Microsoft, Adobe, Salesforce, Oracle, Nielsen, Criteo and several other data companies.[232] Oracle states on its website that there is a "large pool of ID synced users between LiveRamp and the Oracle Data Cloud platform" linking "LiveRamp cookie IDs" to "Oracle Data Cloud cookie profiles".[233] Google and LiveRamp use cookies to "build a match table, which associates LiveRamp RampIDs with Google IDs".[234]

According to the docs, LiveRamp "syncs approximately 2–3 cookies per individual" for each of these third-party companies. This number can vary depending on "the number of devices owned by an individual, the number of browsers they use, how many people are in a given household, whether a user has deleted their browser cookies" and the third-party company. This suggests that LiveRamp identifies two or three different browsers used on different devices for each person.[235] LiveRamp refers to cookie IDs maintained by other third-party companies as "partner cookie IDs".[236] In its global services privacy policy, LiveRamp explains that it may link and associate "LiverRamp cookie" IDs with "partner cookie" IDs.[237]

LiveRamp's "Cookie Sync Tag". To synchronize cookies IDs with LiveRamp, cookie syncing partners can embed the "Cookie Sync Tag" into websites or simply redirect to the tag:[238]

- The tag "leverage[s] standard pixel-based syncing" and "will enable" LiveRamp to "match" a partner's cookie IDs to "other partner cookies, mobile devices, proprietary platform IDs, and RampIDs".
- Using their "online footprint", partners "can fire the LiveRamp tag to initiate a cookie sync with LiveRamp" by redirecting to LiveRamp, sending the following type of HTTP request to LiveRamp:
  https: //idsync.rlcdn.com/<lr_partner_id>.html?partner_uid=<cookie_ID>
- The above HTTP request includes the transmission of a partner cookie ID to LiveRamp, i.e. LiveRamp receives cookie IDs (=personal data) from partners.
- LiveRamp tells its cookie syncing partners that the "cookie sync tag should be placed on as much of your traffic as possible, increasing the amount of traffic synced and the number of cookies you can match with LiveRamp".

---

[228] See e.g. Sincera (2022): The impact of cookie syncing on data leakage and energy consumption. Sincera study commissioned by ID5, November 2022. Online: https://news.id5.io/2022/11/09/id5-and-sincera-study-reveals-damaging-implications-of-cookie-syncing/

[229] p. 48, Christl, Wolfie (2022): Digital Profiling in the Online Gambling Industry. A report on marketing and risk surveillance by the UK gambling firm Sky Betting and Gaming, TransUnion, Adobe, Google, Facebook, Microsoft and other data companies. A report by Cracked Labs commissioned and published by Clean Up Gambling, January 2022. Online: https://crackedlabs.org/en/gambling-data

[230] "Recookiers: allow us to sync with our 400+ cookie integrations": https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [10.9.2023]

[231] https://docs.liveramp.com/safe-haven/en/request-a-reach-estimate.html [7.9.2023]

[232] https://web.archive.org/web/20220523082051/https://liveramp.fr/partenaires/

[233] https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Help/Platform/ManagingTaxonomy/ingest_partners/liveramp_onboard.html [10.9.2023]

[234] https://developers.google.com/ads-data-hub/guides/liveramp-matching [10.9.2023]

[235] https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [10.9.2023]

[236] https://docs.liveramp.com/connect/en/identity-and-identifier-terms-and-concepts.html [6.9.2023]

[237] https://liveramp.com/privacy/service-privacy-policy/ [10.9.2023]

[238] https://docs.liveramp.com/identity/en/implementing-liveramp-s-cookie-sync-tag.html [19.9.2023]

- It also tells its partners that "the more often you sync IDs with LiveRamp, the more of your IDs we'll be able to match to a maintained or derived RampID and potentially tie to a mobile device. Syncing with LiveRamp across a larger footprint, or moving us up in your syncing priority, can lead to higher cookie and mobile match volume".[239]
- It suggests to web publishers who implement LiveRamp's ATS system that they should allow LiveRamp "drop a standard image match pixel" in case they want to "leverage" their "user data to enhance addressability across LiveRamp's match network".[240]
- More broadly, LiveRamp explains that its "Cookie Sync Tag" allows clients to "match" their cookie IDs to partner cookie IDs, mobile device IDs, custom IDs and RampIDs.[241]

LiveRamp's UK and French services privacy policies mention that the company collects "cookie data" or "cookie identifiers". Until 2022, LiveRamp's French website displayed the below list of "Sync Partners".[242] Most likely, this list refers to LiveRamp's cookie/ID syncing partners in France:

Figure 14 © LiveRamp

Linking cookie IDs to other personal identifiers. LiveRamp further maps cookie IDs to other personal identifiers such as mobile device IDs. It explains that "most clients will see the highest number of cross-device linkages cookie-to-cookie, with fewer cookie-to-mobile and mobile-to-mobile linkages". Of course, LiveRamp maps cookie IDs also to RampIDs, its major personal identifier.[243] This is further addressed in the next section.

2.4.3 Sources for other "online" identifiers and links to "offline" identifiers – LiveRamp's "match partners"

As described in section 2.4.1, LiveRamp's identity graph data sources include "offline" data providers for names, postal addresses, email addresses, phone numbers and links between them. As described in section 2.4.2, LiveRamp also maintains personal identifiers for web browsers, which relies on tracking visits to websites at scale. For this purposes, it constantly receives cookie IDs from a network of cookie/ID syncing partners and in turn sends cookie IDs to them. This section addresses a third category of identity graph data sources, which is perhaps the most important, and helps link the "online" identity graph to the "offline" identity graph.

---

[239] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]
[240] https://docs.liveramp.com/privacy-manager/en/ats-extensions.html [10.9.2023]
[241] https://docs.liveramp.com/identity/en/identity-translation.html [13.9.2023]
[242] https://web.archive.org/web/20220523082051/https://liveramp.fr/partenaires/
[243] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023]

LiveRamp's **"match partners"**, which are part of its **"match network"**, provide links between "online" identifiers such as mobile device IDs, cookie IDs and custom IDs (CIDs) on the one hand and "offline" identifiers such as email addresses on the other hand:

- **Links between hashed email addresses and cookie IDs.** LiveRamp's "match partners can monetize match data from their desktop and mobile web pages by implementing the LiveRamp Web Match Tag". The tag "transfers pseudonymized data to LiveRamp's system in the form of a hashed email address / cookie ID linkage". Match partners should add the tag "to all website pages where a user's email addresses can be populated", for example, on "post-registration pages", "post-login pages", "returning-user pages" and "landing page(s) associated with any links in your email newsletters".[244] LiveRamp states to "partner with a large network of websites to pass us logged-in traffic".[245] Match partners can also use the tag to "monetize users who click through their email newsletters" and "monetize[e] email click-throughs". For this purpose, they must include a link in their newsletter that directs users to a "landing page" on their website, which contains "a unique identifier to ID the user".[246] Taken together, as soon as a page on the website of a match partner has access to a user's email address, for example, because the user just registered an account, logged in or clicked on a link in the email newsletter, the match partners sends the hashed email address and LiveRamp's cookie ID to LiveRamp. LiveRamp can then create a new link between an email address and a cookie ID in its identity graph. The "Web Match Tag" sends HTTP requests to LiveRamp that look like:

    https://pippio.com/api/sync?pid={TAG_ID}&it=4&iv={MD5}&it=4&iv={SHA1}&it=4&iv={SHA256}

- **Links between "offline" identifiers and cookie IDs via CIDs.** "EU match partners (such as publishers)" who "cannot send pseudonymized personal data (such as a hashed email address) in a web request" for "security or technical reasons" can use another form of "website data monetization" to send links between cookie IDs and "offline" identifiers such as hashed email addresses to LiveRamp. First, they send files that map custom IDs (CIDs) and "offline" identifiers such as hashed email addresses to LiveRamp. Second, they use the "Customer ID Match Tag" to send cookie IDs and CIDs about "logged-in" websites visitors to LiveRamp. As a result of this two-step process, LiveRamp can create new RampID links between cookie IDs and "offline" identifiers such as email addresses without match partners sending hashed email addresses over the web.[247] This page in the documentation refers to "CIDs" as "Customer IDs" rather than "Custom IDs". It is not entirely clear whether the "Customer IDs" (CIDs) mentioned here are equivalent to the "Custom IDs" (CIDs) described in section 2.2.4. Nevertheless, this may be the way match partners contribute links between hashed email addresses and cookie IDs in Europe and the UK.
- **Links between hashed email addresses and mobile device IDs**. In a similar way, LiveRamp's "match partners can monetize match data from their mobile app registrations and logins by uploading log files to LiveRamp".[248] An extra page in the docs states that "EU match partners" can "monetize the data from their UK and French mobile app registrations and logins by uploading log files to LiveRamp via Amazon S3 or via LiveRamp Connect". To "send mobile app match data to Liveramp", match partners send files that include a mobile app users' hashed email address, their mobile advertising ID (Google AAID or Apple IDFA), the IP address of their device and a timestamp. The name of the uploaded file must contain a country code ("UK" or "FR").[249] LiveRamp states that they "partner with mobile app developers to pass us mobile device IDs", i.e. "Identifiers for Advertisers (IDFAs) and Android Advertising IDs (AAIDs)".[250] It outlines how it has a "mobile device mapping pool", which is "powered" by "traffic" from its "entire match partner network".[251] Taken together, mobile app vendors send hashed email addresses, device IDs and IP addresses of their registered users to LiveRamp. LiveRamp can then create new links between email addresses and mobile device IDs in its identity graph. The fact that the transmitted data includes device IP addresses raises the question of whether LiveRamp also uses IP addresses for identity matching.

[244] https://docs.liveramp.com/connect/en/for-match-partners--implementing-liveramp-s-web-match-tag.html [11.9.2023]
[245] https://docs.liveramp.com/connect/en/liveramp-match-data-sources.html [10.9.2023]
[246] https://docs.liveramp.com/connect/en/for-match-partners--implementing-liveramp-s-web-match-tag.html [11.9.2023]
[247] https://docs.liveramp.com/connect/en/website-data-monetization-through-customer-id-matching.html [11.9.2023]
[248] https://docs.liveramp.com/connect/en/for-match-partners--uploading-mobile-app-files.html [11.9.2023]
[249] https://docs.liveramp.com/connect/en/for-eu-match-partners--uploading-mobile-app-files.html [11.9.2023]
[250] https://docs.liveramp.com/connect/en/liveramp-match-data-sources.html [10.9.2023]
[251] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]

- Put differently, “match partners place pixels on websites and mobile apps and pass” LiveRamp “hashed login events”. LiveRamp “sets a cookie or records the mobile device ID, mapping a unique hash to device/cookie link”.[252]

Selling and buying identity data. LiveRamp often explains that match partners can “monetize” match data. This suggests that match partners sell identity data to LiveRamp. A LiveRamp document from 2021, no longer available online , stated that LiveRamp’s “match network” consists of “paid match partners that send device IDs and cookies linked to hashed PII to LiveRamp, based on observed traffic on their websites, which LiveRamp uses to create or link to an [RampID]”.[253] In 2019, LiveRamp referred to a “network of match partners” as a “combination of the leading online websites and publishers”.[254]

Updating identity graph data over time. LiveRamp explains that it is constantly “constantly dealing with fragmented ID data” within its “match networks”. It receives device IDs “tied to only email hashes, others tied to a name and postal combination, and some with both”. It maintains these fragmented and “sometimes conflicting data points” as “separate entities” by “maintaining multiple RampIDs for a single individual”. Its system “does not automatically assume that separate pieces of PII in a record are tied to the same individual”. Every “RampID corresponds with one or more pieces of PII. Some are stronger than others. Some RampIDs can serve as the building blocks of a full identity and are then merged to form a stronger RampID”. Merging “multiple RampIDs into one only occurs when there is a high degree of confidence that separate identifiers are tied to one person”. The “degree of confidence grows with the number of times we see the two links together”. For example, if LiveRamp receives a RampID for “bob@liveramp/Robert Rich 288 Whitmore St. Oakland” matching a cookie ID, and another “rrch@gmail” RampID matching to the same cookie ID, LiveRamp will not “immediately merge these”.

LiveRamp will merge new information “to an existing individual’s RampID” when it “sees the necessary evidence to confidently tie new information to an existing profile”. LiveRamp will “consolidate” multiple RampIDs into a new RampID “when they are proven to belong to the same strong ID”. Sometimes, it will instead move the “linkages associated with the outdated RampID” to a more recent RampID. The “outdated RampID” will “appear in fewer matches as a result”. Such an update can be caused, for example, by data about “new authenticated logins”.[255]

LiveRamp’s UK services privacy policy states that the company collects personal data from a “variety” of “data sources” it refers to as “online database providers”, which it uses “for identity matching and recognition carried out on behalf” of its clients. LiveRamp explains that it “maintain[s] a network of online Database Provider sources (‘Online Providers’) who provide” the company “with personal data collected from their customers and authenticated users when they visit the Online Providers’ websites and mobile apps. This includes hashed email addresses, in addition to cookie data, mobile IDs, IP addresses and other online identifiers”.[256]

LiveRamp’s French services privacy policy explains that it collects “indirectly identifying data” such as “identifiers linked to your terminals (cookie identifiers, mobile advertising identifiers, etc.) as well as hashed email addresses and associated data (IP address, User Agent, timestamp, URL or app name, etc.)”. LiveRamp uses this data to “link the various data or different terminals (for example, mobile, computer, tablet) relating to the same individual” and provide its “recognition and synchronization solutions” so that its clients are able to target ads adapted to consumer profiles. In addition, the policy mentions “partners” such as “players in the digital and television ecosystem such as publishers of mobile sites and applications”, which it refers to as “Match, OIDL & ATS Partners”.[257] The meaning of the acronym “OIDL” is not clear. It might refer to “Online IdentityLink” partners. “Match” and “OIDL” partners may refer to companies that provide LiveRamp with links between email addresses and device/cookie IDs.

Until 2022, LiveRamp’s French website displayed the following list of “Match, OIDL & ATS Partners”, including Orange, Le Figaro, TF1, Prisma Media and other well-known brands:[258]

---

[252] https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [8.4.2022]
[253] https://liveramp.com/wp-content/uploads/2021/05/Matching-RampID-to-Other-Identifiers.pdf [8.10.2021]
[254] https://liveramp.com/blog/a-primer-on-data-onboarding/ [11.9.2023]
[255] https://docs.liveramp.com/connect/en/how-liveramp-addresses-fragmented-people-based-links.html [10.9.2023]
[256] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]
[257] Original in French, direct quotes in English via Google Translate: https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]
[258] https://web.archive.org/web/20220523082051/https://liveramp.fr/partenaires/

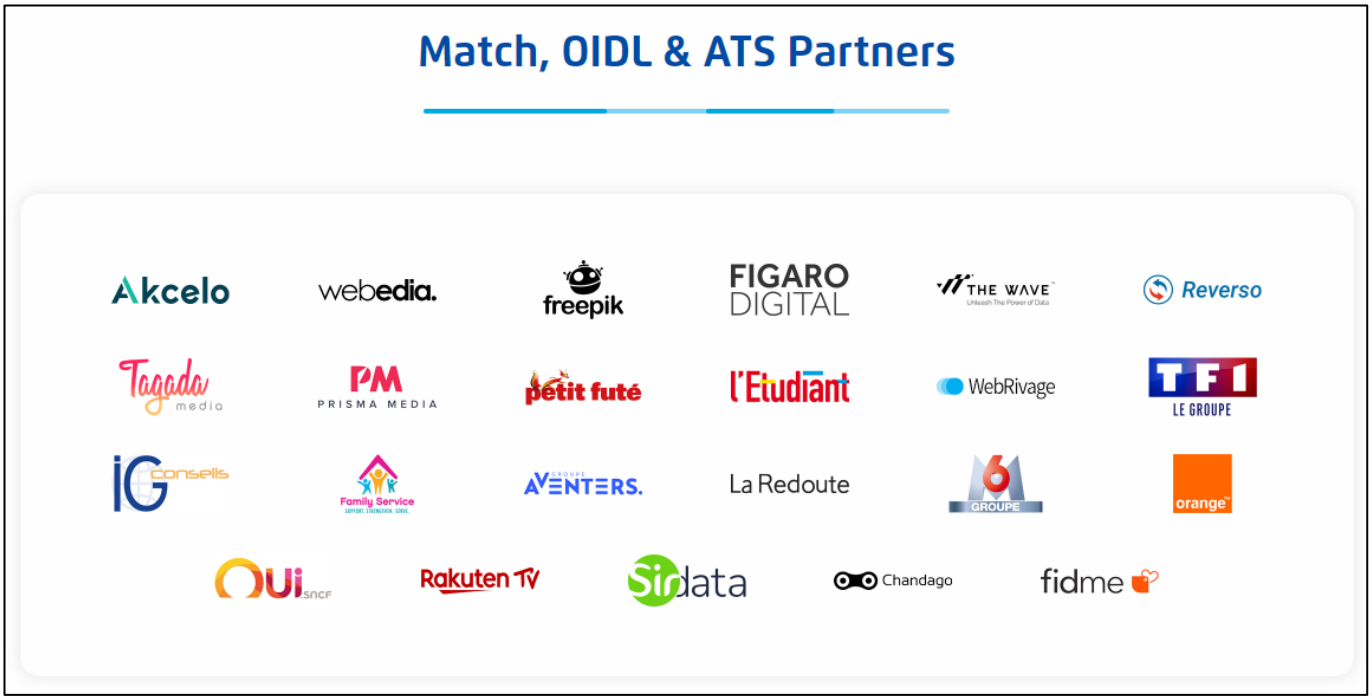


Figure 15 © LiveRamp

LiveRamp's **"Addressability Extension" program**[259] (see section 2.4.1) also provides information about how companies can send this kind of data to LiveRamp. When websites contribute links between email addresses and cookie IDs via the "Addressability Extension Website Tag", LiveRamp "captures hashed email addresses in real-time when a consumer logs in to your website or opens a marketing email where you've deployed our tag", which it uses "to find the consumer's corresponding LiveRamp RampID. Once we find that RampID, we store the linkage between the RampID and the user's cookie ID in our Identity Graph". The hashed "email that is used to perform this lookup is dropped, and never shared or saved to our Identity Graph".[260] There's an extra page in the docs that describes this more in detail, including information about the tag/pixel that "should be placed on your website and called wherever a user's email addresses can be populated".[261]

In addition, data contributors can put an "Addressability Extension Email Tag" directly into the "header" of marketing emails sent to customers, which serves the same purpose of linking email addresses to cookie IDs.[262] To contribute links between email addresses and mobile device IDs, mobile apps can "send log files" of "mobile app registrations and logins" to LiveRamp.[263] LiveRamp then "collects the hashed email addresses tied to mobile device IDs", which it uses "to find the consumer's corresponding LiveRamp RampID. Once we find that RampID, we store the linkage between the RampID and the user's mobile device ID in our graph. The hashed email that is used to perform this lookup is dropped, and never shared or saved to our offline graph."[264] LiveRamp also receives IP addresses of the users' devices and timestamps.[265] It is not clear whether the "Addressability Extension" program is how LiveRamp obtains identity data in Europe today, see section 2.4.1.

Other data providers? Figure 12 indicates that LiveRamp also obtains data from "cross-device linkage partners" and "3rd party graph partners", which suggests that LiveRamp's data sources include other data companies that maintain identity graph systems.

[259] https://docs.liveramp.com/connect/en/addressability-extension.html [10.9.2023]
[260] Ibid.
[261] https://docs.liveramp.com/connect/en/implementing-the-addressability-extension-website-tag.html [11.9.2023]
[262] https://docs.liveramp.com/connect/en/implementing-the-addressability-extension-email-tag.html [11.9.2023]
[263] https://docs.liveramp.com/connect/en/uploading-mobile-app-files-for-addressability-extension.html [11.9.2023]
[264] https://docs.liveramp.com/connect/en/addressability-extension.html [10.9.2023]
[265] https://docs.liveramp.com/connect/en/uploading-mobile-app-files-for-addressability-extension.html [11.9.2023]

2.5 Identity graph use cases and purposes

The previous sections provide extensive information about the basic functionality of LiveRamp's AbiliTec and RampID identity surveillance technology and also describe to some extent how it can be utilized. Section 3 describes further applications. This section provides some additional information about how LiveRamp's identity graph can be utilized. First, it documents data processing activities and purposes as described in LiveRamp's UK services privacy policy. Second, it lists some use cases as described in LiveRamp's software documentation.

2.5.1 Identity graph purposes and processing activities

At one point, LiveRamp's UK services privacy policy[266] states that LiveRamp collects personal data from external data sources "for the purpose of creating and maintaining" its "internal databases".

The policy also contains an additional section about the "purposes for which LiveRamp may use your personal data", which states that the "primary purposes for which LiveRamp will use your personal data is to allow [it] to create and provide solutions to [its] clients and providers to be used for recognition and online targeted advertising". LiveRamp then explains that "recognition" is the process where it uses personal data "stored" in its "databases" for "matching linking data" provided to it by its clients. LiveRamp uses this "recognition process" to "assist" its clients with "online targeted advertising and measurement of advertising effectiveness".

More "specifically", it "may" process information about data subjects for a list of purposes, which are listed in the table below. The table also contains an interpretation of LiveRamp's statements ("interpretation" column):

Purpose mentioned in LiveRamp's UK services privacy policy	Interpretation
"For online interest-based advertising displayed to you by our Distribution Partners at the direction of our clients"	i.e. to allow clients target people with ads based on digital profiles across the digital world (web, mobile apps, platforms etc)
"For use in the measurement and performance of analytics of the effectiveness of our clients' advertising campaigns"	i.e. to allow clients monitor how people respond and interact with ads displayed to them across the digital world
"For enabling our clients and partners to personalise their products and services to you, such as through website and email personalisation or dynamic marketing and advertising optimisation"	i.e. to allow clients personalize their websites, emails and other products/services based on digital profiling
"For enabling our clients and partners to connect your online behavioural preferences across the various browsers and/or devices you use to more accurately market to you"	i.e. to allow clients and partners track, profile and target people across browsers and devices
"For creating modelled audiences to which our clients can market their products and services"	i.e. to allow clients profile people for targeting
"For enabling our clients to associate information they have collected about you with certain identifiers or data made available as part of our products and services to facilitate the delivery of our clients' marketing and advertisements to you", for example, a client "can use our products and services to convert the company's lists from identified names, emails, and/or addresses to de-identified groups of cookie and device IDs maintained by us"	i.e. to allow clients utilize personal data from LiveRamp's identity graph for ad targeting

Figure 16

According to its UK services privacy policy, "additional purposes" LiveRamp processes personal data for include:

- to "analyse, develop, and improve the use, function, and performance of our products and services"
- to "manage the security of our sites, networks, and systems, and to operate our business"

[266] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]

In addition, LiveRamp's UK services privacy policy mentions the following personal data processing activities that rely on LiveRamp's identity graph:[267]

Processing activity mentioned in LiveRamp's UK services privacy policy	Interpretation
"Some of our clients provide us with certain offline personal data (for example, names and contact details of all or a set of their current customers), which we match and link on their behalf to the data held in our Databases"	i.e. LiveRamp processes personal data from its identity graph in order to match and link it with personal data provided by clients
"We also receive datasets from additional third parties who hold their customers' personal data ('Data Marketplace Sellers'), match this to online identifiers using our Databases, and then make the resulting online marketing audience available on our 'Data Marketplace' to our clients who wish to carry out marketing ('Data Marketplace Buyers')"	i.e. LiveRamp processes personal data from its identity graph in order to help third parties sell personal data via its "data marketplace" (see section 3.1.2)
"We also assist our clients in distributing the matched online data and audiences to third parties ('Distribution Partners') who use it in the delivery of our clients' online targeted advertising."	i.e. LiveRamp processes personal data from its identity graph in order to help clients transmit personal data to third parties
"For example, a client would use our services to better serve advertisements to their customers. Such client sends us a file of their customer data, which we then match to our data. We then delete the original client data and produce resulting matches that are pseudonymised (all directly identifiable personal data is removed and replaced with our proprietary identifiers called 'RampIDs'). We exchange this matched RampID data list (the audience) with our Distribution Partners, who then facilitate the sending or display of the client's advertisements to those consumers"	This represents a more detailed description of the first and the third processing activity listed in this table. LiveRamp processes personal data from its identity graph in order to match and link it with personal data provided by clients. Subsequently, LiveRamp processes personal data from its identity graph to transmit (or "exchange") personal data to third parties

Figure 17

2.5.2 Identity graph uses cases according to the docs

Non-exhausyive list of use cases for LiveRamp's identity graph according to LiveRamp's software documentation (emphasis by the author of this report):

- So-called "mapping files" (see section 2.2.5.5) can be used for:[268]
  - "**recognizing non-logged in users** on your website for site personalization"
  - "powering **targeting and measurement** for your application/platform users"
  - "**improving monetization** by expanding the device reach of your segments"
- LiveRamp's "Real-Time Identity Service Tag" (see section 2.2.5.4) can be used to:[269]
  - "**access people-based data immediately at the time of impression** for your own **measurement and personalization** products", "a device you don't recognize could be matched, through a RampID, to a known device, making that impression **actionable and measurable**"
  - "build **ad traffic logs keyed to RampIDs** in real-time"
  - "**personalize** content for your visitors […] **The RampID can then be used to look up segment data, or other known data on the individual** for site-personalization"
- LiveRamp's "File-Based Recognition Workflow" that allows clients upload files with identifiers and receive files where the uploaded identifiers are replaced with RampIDs (see section 2.2.5.1) can be used for the following purpose:[270]
  - "Once your file contains RampIDs, **you can then tie the original dataset to any other source you have linked to RampID**. General use cases for this workflow include **measurement, targeting, exposure, conversion, and more**"
- Segment data uploaded to LiveRamp's "Connect" platform via "onboarding" (see section 2.2.5.3) can be used to:[271]
  - "group your records into segments based on certain attributes so you can distribute those segments to one of LiveRamp's partners, typically for **targeting, measurement, or personalization**"

[267] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023]
[268] https://docs.liveramp.com/identity/en/rampid-mapping-files.html [7.9.2023]
[269] https://docs.liveramp.com/identity/en/implementing-liveramp-s-real-time-identity-service-tag.html [7.9.2023]
[270] https://docs.liveramp.com/connect/en/file-based-recognition-workflow.html [7.9.2023]
[271] https://docs.liveramp.com/connect/en/types-of-data-that-can-be-included-in-files.html [17.9.2023]

- The “permitted uses cases” for data sold via LiveRamp’s “data marketplace” (see section 3.1.2) include:[272]
  - “digital ad targeting”
  - “audience extension”
  - “campaign analytics”
  - “tv targeting”
  - “measurement”

2.5.3 Identity graph use cases as seen by a LiveRamp partner

According to promotional material from a partner company, LiveRamp’s identity graph systems allow companies to “bring together data from the wide range of marketing and non-marketing activities that brands leverage — campaign impression data from display, video, mobile and search, website traffic, traditional advertising impressions, email, direct mail, survey panel data, purchase data and 3rd party data — and connect it all to a unique person ID”. Using LiveRamp’s identity graph system, the partner company “can create a comprehensive view of interactions at the person and household level”. The chart below illustrates how this partner company sees the role of LiveRamp:[273]

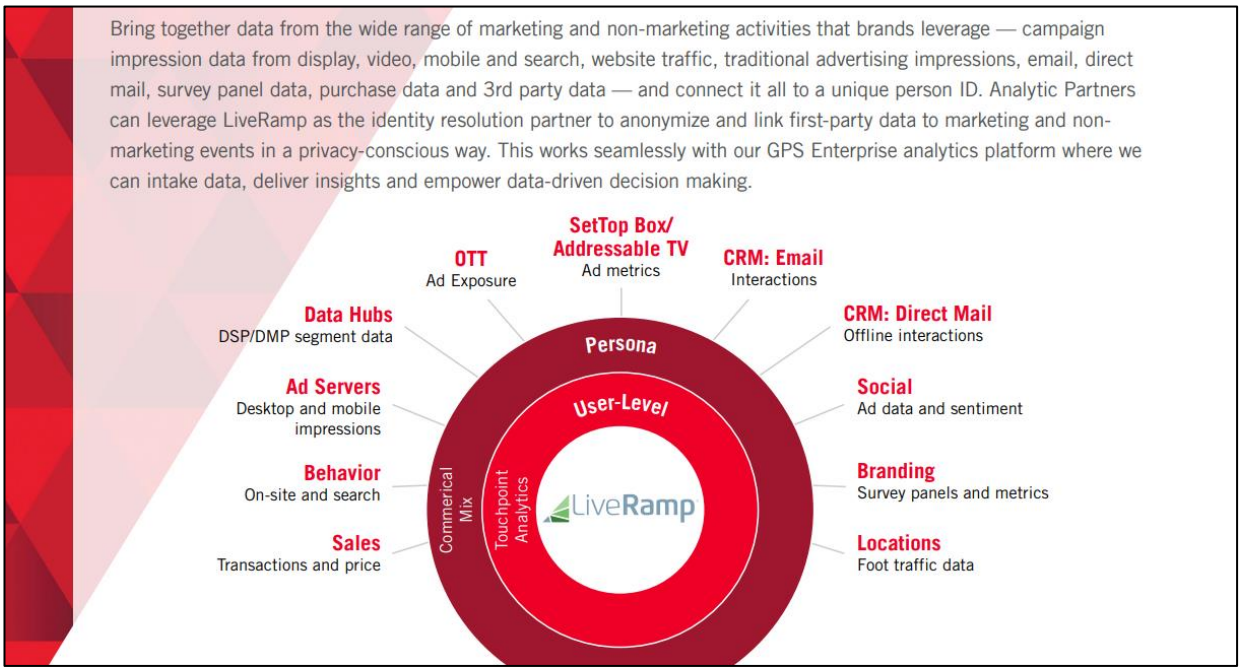


Figure 18 © Analytic Partners

(“DSP/DMP segment data” from “data hubs” refers to segments, i.e. lists of identifiers referring to people with certain characteristics, provided by third-party data brokers)

2.6 LiveRamp’s identity graph in its UK and French services privacy policies

The previous sections describe how LiveRamp collects and processes personal data to create and maintain its AbiliTec and RampID systems and provide services that rely on it, mostly based on an analysis of software documentation. Some sections, in particular section 2.4 on LiveRamp’s identity graph sources, also address the services privacy policies from LiveRamp’s UK and French websites.[274]

Both policies contain ambiguous statements, which are difficult to interpret and thus leave open questions, particularly in combination with the data practices documented in this report. While a comprehensive legal analysis of LiveRamp’s personal data processing activities is beyond the scope of this report, this section briefly points out some issues mentioned in LiveRamp’s

[272] https://docs.liveramp.com/connect/en/data-marketplace-permitted-use-cases.html [13.4.2022]
[273] https://www.mafonavigator.de/directories/media/1/pdf-2260.pdf [17.9.2023]
[274] https://liveramp.uk/privacy/service-privacy-policy/ [5.9.2023], https://liveramp.fr/politique-confidentialite-produits-services/politique-de-confidentialite-de-nos-produits-et-services-2/ [6.9.2023]

services privacy policies. Any statements quoted from the French services privacy policy rely on an automated translation via Google Translate.

2.6.1 Data controllership

The UK services privacy policy states that LiveRamp is a data controller "where" it "collect[s]" personal data from "database providers" and "hold[s] it in the database". It explains that it is a data processor on behalf of its clients for almost any other personal data processing including for the "matching process". This is a questionable claim, because matching often involves processing personal data from LiveRamp's identity graph.

The French policy states, more broadly, that LiveRamp is a data controller for "build[ing]" its "offline and online data repositories" and for data processing that is carried out to "provide solutions" for "recognition", "pseudonymization" and "synchronization". Once its clients' data is "pseudonymized" and "synchronized" via "recognition", LiveRamp also sees itself as a data processor on behalf of its clients, according to the French policy.

As detailed in section 3.3.3, LiveRamp's sees itself, its clients and other data companies as joint controllers in the context of its "Authenticated Traffic Solution" (ATS) product. While the French services privacy policy reflects this, the UK policy does not mention it at all.

The claims laid out in its policies raise the question whether LiveRamp could be considered a (joint) controller for some of the many other data processing activities documented in this report.

2.6.2 Legal basis

The UK services privacy policy mentions "consent" only once. LiveRamp explains it relies on "consent as the lawful basis for processing" to "the extent that the collection of personal data from an Online Provider involved the placement or reading of a cookie (or similar technologies)". The company states that personal data in its "databases" is processed on the basis of its "legitimate interests".

The French policy often mentions the term "consent and explains that it relies on it as a legal basis where it is "data controller" for any "data relating to cookies and pixel", "pseudonymous identifiers generated as part of ATS", and "TV exposure data". Certain data processing related to clients who promote products via email or SMS is subject to "consent". "Match partners" must allow users to some means to "consent" to data processing. When LiveRamp shares pseudonymous data with "sync partners" and "Match, OIDL & ATS Partners" for the "sole purpose of enabling" it "to synchronize with them", this is also subject to "consent". This points to the fact that obtaining personal data from third parties often also involves sharing personal identifiers with them in order to synchronize identifiers. The French policy also mentions that LiveRamp "complies with the specifications and policies" of the IAB's TCF and points to its TCF vendor number. This is further addressed in section 2.6.4 and not mentioned in the UK policy. The French policy states that LiveRamp relies on its "legitimate interests" to process any other personal data which is "essential" to operate its "recognition and synchronization solutions" and which is not subject to consent, as summarized above.

The claims laid out in these policies raise several questions about whether LiveRamp really has valid consent in all cases where it claims to rely on consent, and whether it can really rely on its legitimate interests for its identity graph processing.

2.6.3 Data retention

The UK services privacy policy states that LiveRamp retains "online information" for "up to six (6) months or twelve (12) months, depending on the data and the applicable purpose(s)", except for "device identifiers which may be retained until necessary for the applicable purposes". Similarly, "offline information collected from Database Providers will be retained while there's a continuing need to keep it for the applicable purposes".

The French policy states that LiveRamp retains cookie IDs for "12 months", mobile IDs for "240 days" and "associated data" related to cookie and pixels for "12 months". Most other personal data for its identity graph will be retained "2 years" from its "last interaction with the data concerned". LiveRamp also explains that it does "not store" pseudonymous identifiers generated as part of its ATS product.

2.6.4 IAB "Transparency & Consent Framework" (TCF)

The IAB's "Transparency & Consent Framework" (TCF) also appears to be relevant for the legal justification of LiveRamp's personal data processing on the web, and perhaps also in some mobile app contexts. A page in the docs[275] explains that LiveRamp "released TCF 2.0 functionality for EU Pixel Servers" in 2020. Since then, "All pixel-based events" are "subject to TCF 2.0 when they originate in the EU markets that LiveRamp operates in". It will be "enforcing this standard on processing all inbound traffic". On this page, LiveRamp states that it requires TCF 2.0 consent that includes "LiveRamp as a vendor" for a number of "purposes", "special purposes" and "features" as defined by the TCF.[276]

The following figure shows LiveRamp's entry in the official TCF vendor list file that is accessible via https://vendor-list.consensu.org/v2/vendor-list.json, as of September 15, 2023: [277]

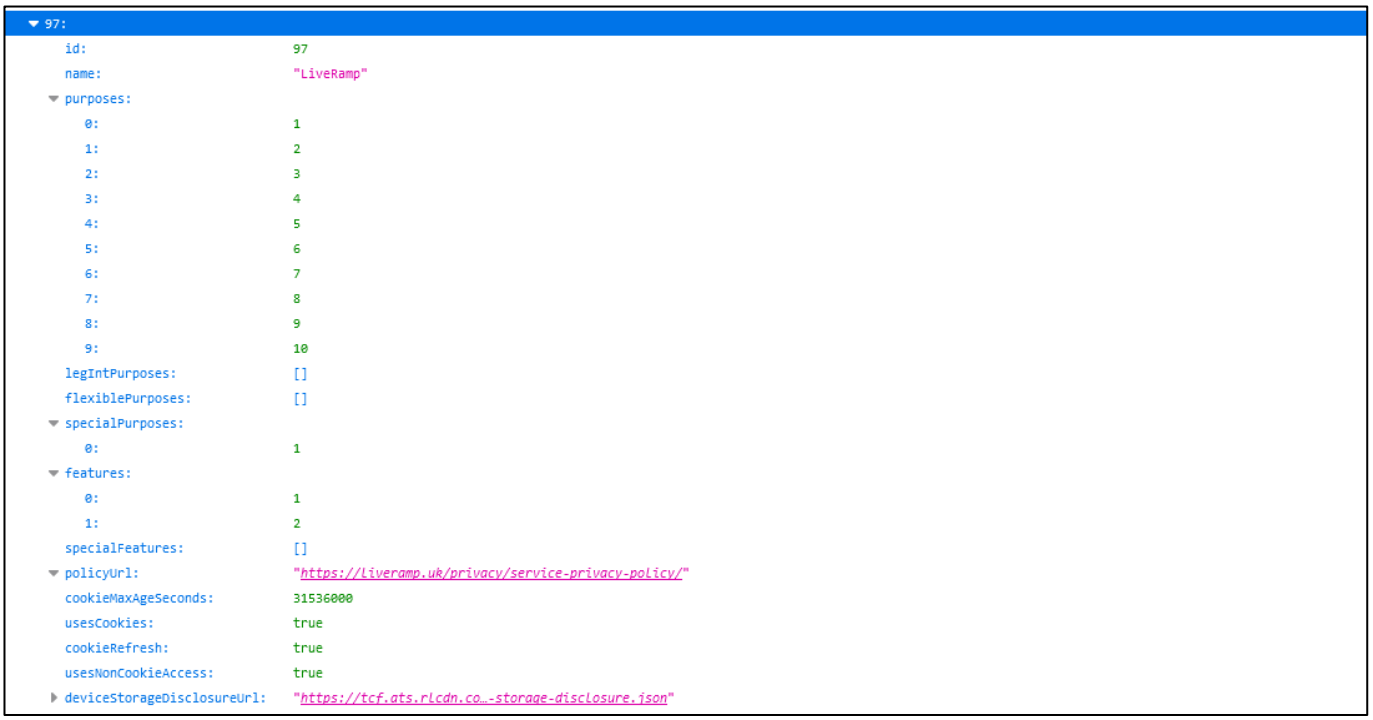


Figure 19

The vendor record shows that LiveRamp requires "consent" to the following "purposes", "special purposes" and "features":

- Purpose 1 - Store and/or access information on a device
- Purpose 2 - Select basic ads
- Purpose 3 - Create a personalised ads profile
- Purpose 4 - Select personalised ads
- Purpose 5 - Create a personalised content profile
- Purpose 6 - Select personalised content
- Purpose 7 - Measure ad performance
- Purpose 8 - Measure content performance
- Purpose 9 - Apply market research to generate audience insights
- Purpose 10 - Develop and improve products
- Special Purpose 1 - Ensure security, prevent fraud, and debug
- Feature 1 - Match and combine offline data sources
- Feature 2 - Link different devices

[275] https://docs.liveramp.com/connect/en/announcing-support-for-tcf-2-0-functionality-for-eu-pixel-servers--9-3-20-.html [12.4.2022]
[276] https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ [28.6.2022]
[277] IAB vendorlist file version 215: https://vendor-list.consensu.org/v2/vendor-list.json [15.9.2023]

As the above record from the TCF vendor list shows, LiveRamp's TCF privacy policy link for all European users points to the UK services privacy policy.

2.7 How LiveRamp captures identity graph data

While section 2.4 examines in detail how LiveRamp obtains data for its identity graph databases, the following explanations provided by LiveRamp offer further insight into how the system works (emphasis by the author of this report):[278]

"Fairly regularly, LiveRamp will maintain multiple RampIDs for a single, real-world individual. This occurs when LiveRamp has not yet resolved different pieces of PII to a single individual; each piece of PII is therefore assigned its own RampIDs. We follow this approach to prioritize accuracy over optics; ideally LiveRamp will always have all PII touchpoints merged for an individual, but **our algorithms will only merge this data when we are extremely confident they are tied to the same individual**. For example, say LiveRamp has RampID XY123 tied to the email bob@bob.com and postal address Bob Lincoln 123 Street Cincinnati, OH. If Bob gets a new email, **LiveRamp will need to see that email associated with Bob's postal address a certain number of times before associating the new email to Bob's existing RampID**. In the meantime, the new email would be assigned a new RampID, Xi456. After LiveRamp has seen the necessary touchpoints to accurately tie this new address to the existing profile, the new address will be updated to match to the existing XY123 RampID for Bob. **LiveRamp's massive online and offline footprint allows us to do this both quickly and accurately**."	"LiveRamp often manages multiple RampIDs for an individual. **This is because people are dynamic**: they move houses, change jobs, switch phones, share computers, and upgrade their tech. In the U.S., in 2018 alone, there were 36 M residential moves, 4 M births, 2.2 M marriages, and almost 800 K divorces. Each of these events might create a new PII touchpoint. When we observe a new piece of PII, we create a RampID for that touchpoint. **Over time, each of these events builds a more complete picture of that person's identity**. But **until we are able to confidently recognize and prove that these new PII touchpoints are tied to that one individual**, we might associate multiple RampIDs with that individual's data. **Once we have a high degree of confidence that the new touchpoints are tied to that individual**, we merge those RampIDs into a single maintained RampID. **Thanks to our massive online and offline footprint**, we are able to successfully do this more accurately and faster than any alternative."

Figure 20

3. Applications for LiveRamp's identity graph systems

LiveRamp's identity graph systems enable and facilitate extensive personal data processing by its clients, who can utilize them to recognize, track, profile and target people across browsers, devices, websites, apps, platforms, customer databases and life contexts, according to the findings of the previous sections and the company's UK services privacy policy (see section 2.5). Clients can utilize LiveRamp's identity graph systems to monitor how people act in response to ads and to personalize their websites, emails and other services. They can combine personal data across different sources, send it to other data companies, buy additional personal data from third parties or sell it themselves

While section 2 examines and documents the basic functionality of LiveRamp's AbiliTec and RampID identity surveillance technology, this section explores further applications that rely on it. As such, this section also provides further information about the nature and scale of personal data processing in the context of LiveRamp's identity graph systems.

Sections 2.1.4 and 2.1.6 describe how clients can query the AbiliTec system and some "use cases" for it. While it is not entirely clear whether and how European clients can directly utilize LiveRamp's AbiliTec system, they can certainly utilize it via the RampID system, which builds on top of it. Sections 2.2.5 and 2.3.2 show that clients can query and utilize the RampID system in the following ways:

[278] https://docs.liveramp.com/connect/en/interpreting-rampid,-liveramp-s-people-based-identifier.html [6.9.2023], https://docs.liveramp.com/connect/en/file-output-options-for-file-based-recognition-workflows.html [7.9.2023]

- LiveRamp's clients can upload files with consumer records that contain names, postal addresses, email addresses, phone numbers and other personal attributes about these persons. LiveRamp "recognizes" the persons based on the uploaded identifiers and returns files where the uploaded identifiers are replaced with pseudonymous RampIDs.
- In a similar way, clients can upload or "onboard" consumer records to LiveRamp's cloud-based "Connect" platform. They can upload, for example, entire customer databases or purchase transaction records. Once again, LiveRamp "recognizes" the corresponding persons and provides functionality for further analysis. Clients can organize the "onboarded" data into "fields" and "segments", the latter of which are lists of identifiers referring to people with certain characteristics. Subsequently, clients can send these segments to hundreds of adtech firms, platforms and other third-party companies, for example, for ad targeting. LiveRamp synchronizes personal identifiers across all involved parties based on its identity graph systems and thus facilitates the exchange of other personal data about the affected persons across all involved parties. This is further detailed in section 3.1.1.
- Clients can also use LiveRamp's tracking "tags" to collect personal data about website visitors and mobile app users. They can "attach" tracking tags to digital ads and thus track people who interact with these ads somewhere in the digital world. LiveRamp can "recognize" anonymous website visitors, app users or people who interact with ads in real time and return the corresponding RampIDs, which can then be used for purposes such as personalization and measurement. Clients can also use LiveRamp's tracking tags to automatically ingest the recorded data into "Connect" and then use the platform for further analysis, segmentation and distribution to other companies.
- When clients use LiveRamp's tracking tags or certain other "Connect" functionality, they can receive "mapping" log files, which contain detailed records that map cookie IDs or mobile device IDs to the corresponding RampIDs.
- Clients can also get direct real-time access to LiveRamp's identity graph through the "RampID API". When they send names, postal addresses, email addresses and phone numbers to LiveRamp, LiveRamp "recognizes" the corresponding persons and returns pseudonymous RampIDs.
- LiveRamp's identity graph systems still appear to significantly rely on personal identifiers processed via third-party cookies in the browser to track and target people on the web. LiveRamp incentivizes clients to use its 'cookie syncing' tag, which not only helps to link cookie IDs with partner cookie IDs across many companies, but also improves the ability to match cookie IDs to mobile device IDs and RampIDs.

These examples show that companies can utilize LiveRamp's identity graph systems both within the company's "Connect" platform (e.g. "onboarding", tags, segmentation, distribution) and independently from it (e.g. "file-based recognition", tags, "mapping" log files, RampID API).

Section 3.1 further examines how clients can utilize LiveRamp's identity graph systems in the company's "Connect" platform, from distributing consumer records to Google, Facebook and other adtech and data companies to selling and buying data via LiveRamp's "data marketplace". Section 3.2 explores how RampIDs can serve as "universal" identifiers in the broader data and adtech industry, from the transmission of billions of RampIDs in the RTB bidstream in digital advertising per day to Google utilizing RampIDs as a "join key" between its advertising clients' data and its own massive behavioral data sets. Section 3.3 investigates LiveRamp's "Authenticated Traffic Solution" (ATS) product, a thin compliance layer based on "identity envelopes" that enables publishers to push email-based RampIDs into the broader data and adtech ecosystem.

3.1 Utilizing identity surveillance in LiveRamp's "Connect" platform

This section further examines how companies can utilize LiveRamp's identity graph systems within the company's cloud-based "Connect" platform,[279] which enables clients to upload personal data to LiveRamp (as detailed in sections 2.2.5.1 and 2.2.5.3) and then analyze it, create segments, obtain third-party data from LiveRamp's data marketplace, further distribute personal data to hundreds of other companies or sell it.

3.1.1 Distributing data to "destinations"

As soon as LiveRamp's clients have uploaded or otherwise ingested consumer records into the "Connect" platform, they can "distribute" it to companies which LiveRamp refers to as "destinations".[280] LiveRamp enables clients to distribute data to "more

[279] https://docs.liveramp.com/connect/index.html [6.9.2023]
[280] https://docs.liveramp.com/connect/en/distributing-data.html [12.9.2023]

than 500" destinations,[281] for example, to other data companies, adtech firms, marketing intermediaries, platforms and publishers.[282] This includes Google, Facebook, TikTok, LinkedIn, Twitter, Pinterest, Snapchat, Amazon, Yahoo, Adobe, Salesforce, Microsoft's Xandr, The Trade Desk, Criteo, Pubmatic and many other firms.[283]

3.1.1.1 Sending lists of RampIDs, cookie/device IDs and other identifiers

The data that is processed in "Connect" and can be distributed to destinations can consist of "segments", which are lists of identifiers referring to people with certain characteristics (see section 2.2.5.3).

A "segment" stored by a client in the "Connect" platform can, for example, consist of a list of 5,000 RampIDs referring to persons who have been categorized as "Porsche owners", "new parents" or "interested in payday loans". To distribute such a list of identifiers to a destination for targeted advertising, LiveRamp has to make sure that the included identifiers are "understood" by the destination. The destination must know, which persons to target.

As the following graphic shows, LiveRamp can send, for example a list of cookie IDs, mobile device IDs (Apple IDFA, Google AAID) or RampIDs to a destination:[284]

Figure 21 © LiveRamp

Different destinations accept different identifiers. Clients can configure which identifiers they want to send to a destination.[285] When a destination receives cookie IDs, it can identify and single out the persons to target based on cookie/ID syncing with LiveRamp. When a destination receives mobile device IDs, it can identify and single out the persons to target without any further help from LiveRamp, because mobile device IDs such as Apple's IDFA and Google's AAID are known as universal personal identifiers for mobile devices. When a destination receives RampIDs, it must use LiveRamp's RampID services in order to be able to identify and single out the persons for targeting.

RampIDs are the "default" identifier for destinations that accept them.[286] LiveRamp recommends its clients to "keep RampID selected" in order to "maximize" their "reach and match rates".[287]

Cookie IDs. When LiveRamp sends cookie IDs to a destination, the client can choose from two options:[288]

- **Device matching** "uses" LiveRamp's "partner cookie mapping to deliver only the destination cookie that matches to the input partner cookie (one cookie in, one cookie out when a linked cookie is available)", i.e. LiveRamp sends only a single linked cookie ID to the destination, if available.

[281] https://docs.liveramp.com/connect/en/onboarding-your-data.html [6.9.2023]
[282] https://partner-directory.liveramp.com/ [7.9.2023]
[283] https://docs.liveramp.com/connect/en/platform-specific-distribution-information.html [12.9.2023]
[284] https://docs.liveramp.com/connect/en/activate-a-new-destination-account.html [12.9.2023]
[285] Ibid.
[286] https://docs.liveramp.com/connect/en/announcement--rampid-now-the-default-identifier-in-certain-destination-accounts--9-15-22-.html []
[287] https://docs.liveramp.com/connect/en/activate-a-new-destination-account.html [12.9.2023]
[288] https://docs.liveramp.com/connect/en/precision-levels.html [12.9.2023]

- **Individual matching** "uses the links that each cookie has to individuals" in LiveRamp's "online graph to find all the cookies (and therefore devices) we believe are associated with a given individual (one cookie in, potentially many cookies out)", i.e. LiveRamp sends all cookie IDs it has linked to a given individual to the destination.

Mobile device IDs. Similar options are available when LiveRamp sends mobile device IDs to a destination:[289]

- **Device matching** "simply passes through the mobile device IDs that were included in the input data (one MAID in, the same MAID out)", i.e. LiveRamp sends the same mobile device IDs that a client has ingested into the "Connect" platform to the destination.
- **Individual matching** "utilizes the links that each mobile device ID has to records in our online graph to find all the mobile device IDs (and therefore devices) we believe are associated with a given individual (one MAID in, potentially many MAIDs out)", i.e. LiveRamp sends all mobile device IDs it has linked to a given individual to the destination.

In case of "individual matching", LiveRamp uses its full "online" identity graph to send not only single cookie or device IDs to a destination, but all cookie or device IDs it has linked to the person in its identity graph. As such, LiveRamp enriches the "input" identity data based on its identity graph data. In addition to RampIDs, cookie IDs and device IDs, LiveRamp can send other identifiers to certain destinations:

- **Custom IDs.** LiveRamp can send custom IDs (CIDs) to certain destinations.[290]
- **Hashed "offline" information such as hashed email addresses.** For certain destinations, LiveRamp provides a "Direct-to-Platform integration", which it also refers to as a "PII Passthrough" integration. In this case, it sends "hashed PII in a privacy-safe and compliant manner" to the destination "without performing matching (or any leveraging of our Identity Graph)", which then allows the destination to match the hashed "offline" information to its "universe of users".[291]

"Refreshing" destination data. LiveRamp does not only send the data once but constantly keeps "refreshing" the data that is being sent to the destination company. To "ensure that there is always an up-to-date pool of users in the distribution", it "continuously updates data distributed to a particular destination, including new devices (cookies and mobile devices) seen in" LiveRamp's "match network".[292] These "refreshes" can be "triggered" in a number of ways:[293]

- Whenever clients upload new data for "existing segments"
- Whenever clients add new "segments"
- Whenever clients choose to manually "resend" the data
- Whenever "5 days have passed since the last data refresh" for "cookie-based destinations"
- Whenever "15 days have passed since the last data refresh" for "mobile device ID-based destinations"

These "refreshes" can include the following data:[294]

- "New devices", i.e. "devices associated with new records that have been added to the original distribution"
- "New associated devices", i.e. "devices [LiveRamp has] seen for the first time in [its] match network since the last refresh"
- "Backlog data", i.e. "a portion of [a client's] existing data so that the destination partner doesn't expire that data (such as a cookie) because they haven't seen it for a certain amount of time"

"Destinations" available in France and the UK? Until 2022, LiveRamp's UK website provided lists of "standard destinations", "data marketplace destinations" and "data sources for measurement" (the latter of which are also considered "destinations", see section 3.1.3) that are available in France and the UK.[295]

---

[289] Ibid.
[290] Ibid.
[291] https://docs.liveramp.com/connect/en/direct-to-platform-destination-integrations.html [12.9.2023]
[292] https://docs.liveramp.com/connect/en/how-liveramp-refreshes-distributed-data.html [12.9.2023]
[293] Ibid.
[294] Ibid.
[295] https://web.archive.org/web/20220703093145/https://liveramp.uk/partners/

Reliance on LiveRamp's identity graph systems. Taken together, LiveRamp provides a lot of functionality to send personal data to "destination" data companies and constantly keep it updated. While clients initiate these personal data transmissions, they rely on LiveRamp's identity graph data and other functionality provided by LiveRamp. Its identity graph enables and facilitates these personal data transmissions. Clients could not transmit the data to these destinations, some of which match the transmitted data to their own records about billions of people, without LiveRamp's massive efforts to maintain its identity graph and link the transmitted data with personal data processed by destinations.

3.1.1.2 Sending lists of identifiers to "onboarding integration partners"

As LiveRamp is one of only a few players globally that provides comprehensive "onboarding" functionality, which allows companies to upload consumer records that contain names, postal addresses, email addresses and phone numbers and then use it in the broader adtech and data ecosystem, LiveRamp allows "onboarding integration partners" and "resellers" to utilize and resell its "onboarding" technology.[296] It is not clear how many integration partners and resellers do so and whether large companies are among them. Onboarding integration partners directly receive files from LiveRamp that contain "identifiers, such as cookies or mobile device IDs, tied to segment IDs".[297]

Oracle provides a "LiveRamp Offline Match Integration" that enables its clients to use LiveRamp's "onboarding" technology to "onboard customer data linked to personally identifiable information" and then "leverage the large pool of ID synced users between LiveRamp and the Oracle Data Cloud platform".[298]

3.1.1.3 Sending lists of identifiers to Facebook

LiveRamp provides several data integration options with Facebook.[299] It describes one of these options, the "managed integration" with Facebook, as follows:[300]

Uses: Targeting only. **Integration Method:** In this type of integration, your first-party data distributions are delivered into LiveRamp's Facebook ad account, and then shared by LiveRamp to your Facebook ad account. **Matching Process:** LiveRamp matches your data to RampIDs, finds all possible Facebook CIDs that are tied to the same RampID, and delivers those matched CIDs via an API to LiveRamp's Business Manager within Facebook. Facebook then uses a mapping file it has generated in its backend to look up the CIDs it received and matches them to their Facebook IDs.	**MATCHING STEPS** 1) On a quarterly basis, LiveRamp sends Facebook a mapping file of pre-approved-for-marketing hashed PII tied to our Facebook CIDs (also referred to as "ExternIDs" by Facebook). Facebook then generates a mapping in their backend of ExternID to Facebook ID, which allows us to send only ExternIDs when delivering data. 2) When first-party customer data are uploaded, LiveRamp matches that data to RampIDs, finds all possible Facebook CIDs that are tied to the same RampID, and delivers those matched CIDs via an API to LiveRamp's Business Manager within Facebook. 3) Facebook then uses the mapping file it generated in its backend to look up the CIDs (ExternIDs) it received and matches them to their Facebook IDs. 4) LiveRamp then shares the Custom Audience from a LiveRamp-owned ad account to the customer's ad account.

Figure 22

This description suggests that:

- LiveRamp sends Facebook a file that maps hashed "PII" (such as hashed email addresses) tied to "custom IDs" (CIDs) on a quarterly basis. Based on the hashed "PII", Facebook recognizes people and creates a database that maps LiveRamp's CIDs to Facebook user IDs. The file sent to Facebook potentially contains personal data about many people, but is restricted to records that are "pre-approved-for-marketing". It is not clear what this means.
- LiveRamp's clients send records about consumers that contain identifying information to LiveRamp.

[296] https://docs.liveramp.com/connect/en/reseller-onboarding.html [7.9.2023]
[297] https://docs.liveramp.com/connect/en/data-delivery-guide-for-onboarding-integration-partners.html [13.9.2023]
[298] https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/ManagingTaxonomy/ingest_partners/liveramp_onboard.html [14.9.2023]
[299] https://docs.liveramp.com/connect/en/distribute-data-to-facebook.html [13.9.2023]
[300] https://docs.liveramp.com/connect/en/facebook-destination-account-integration-options.html [12.9.2023]

- LiveRamp creates RampIDs based on recognizing the corresponding persons, finds "all possible Facebook CIDs that are tied to the same RampID" and sends those "matched CIDs" to Facebook.
- Facebook utilizes the database that maps LiveRamp's CIDs to Facebook users IDs to recognize the corresponding Facebook users and creates a "Custom Audience" for ad targeting.

It is not entirely clear whether this functionality is fully available in Europe. On the page that describes this Facebook integration, LiveRamp emphasizes that clients must "pick the integration that's labeled for [their] country or region (US, FR, UK, DE, LATAM, etc.)". This suggests that at least some Facebook integration functionality is available in France, Germany and the UK. LiveRamp states that while its "regular Direct Integration is only available for U.S. first-party data", the "managed integration" described above can be used for "non-U.S. first-party data".[301]

3.1.1.4 Sending lists of identifiers to Google

LiveRamp also provides several data integration options with Google. It describes one of these options as follows:[302]

- When distributing data from the "Connect" platform to Google via "Customer Match", LiveRamp can send "offline identifiers" such as "email, name and postal address, and phone number" to Google. As this is a "Direct to Platform (PII passthrough) integration", LiveRamps explains to "pass the PII directly through in a privacy-safe and compliant manner, with no leveraging of our Identity Graph". Notably, LiveRamp states that data stored in "Connect" based on "RampIDs that have been generated from PII" can also be sent to Google via "Customer Match". Perhaps LiveRamp retains the "offline" identifiers its clients upload to "Connect" in order to be able to send them to Google.[303]
- **Identity enrichment.** In addition, LiveRamp offers to "use Data Append to increase your match rate within Google Customer Match by leveraging our Identity Graph to add additional emails to your uploaded data".[304] As such, LiveRamp's clients can send names, postal addresses, email addresses or phone numbers to LiveRamp, which in turn retrieves additional email addresses linked to the same person from its identity graph and sends these additional email addresses in hashed format to Google.

It is not clear to what extent these integrations are available in Europe, France and the UK.

3.1.2 LiveRamp's "data marketplace"

In the same way LiveRamp's clients can upload or otherwise ingest consumer records into the "Connect" platform, they can become "data sellers",[305] or in turn buy data from those who sell it.[306] Data sellers, some of which are also referred to as "data providers", can sell "segments",[307] i.e. lists of identifiers referring to people with certain characteristics (see section 2.2.5.3).

LiveRamp claims to provide "multi-sourced insight into approximately 700 million consumers worldwide" from "more than 150 data providers" through its "data marketplace".[308] A screenshot in LiveRamp's docs suggests that these data providers sell 234,533 different segments via LiveRamp's data marketplace.[309]

3.1.2.1 Selling and buying data

According to LiveRamp, "data marketplace data can be sold" in the US, Australia, New Zealand, France and in the UK.[310] In 2022, LiveRamp's UK website provided lists of third-party "data providers" available in the UK and France. Third-party data providers available in the UK included data brokers and other companies such as Acxiom, Experian, IRi, IHS Markit, Kantar, Mastercard, Adara and Weborama. Third-party data providers available in France additionally included some smaller data

[301] Ibid.
[302] https://docs.liveramp.com/connect/en/distribute-data-to-google.html [13.9.2023]
[303] https://docs.liveramp.com/connect/en/distribute-first-party-data-to-google.html [13.9.2023]
[304] Ibid.
[305] https://docs.liveramp.com/connect/en/selling-data-with-the-data-marketplace.html [13.9.2023]
[306] https://docs.liveramp.com/connect/en/buying-data-or-services-from-the-data-marketplace.html [13.9.2023]
[307] https://docs.liveramp.com/connect/en/selling-data-with-the-data-marketplace.html [13.9.2023]
[308] https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm [5.9.2023]
[309] https://docs.liveramp.com/connect/en/available-columns-on-the-data-marketplace---buy-segment-data-page.html [13.9.2023]
[310] https://docs.liveramp.com/connect/en/countries-where-data-marketplace-data-can-be-sold.html [13.9.2023]

brokers such as Factual, AlikeAudience, Lifesight, start.io and Sharethis.[311] When uploading data in order to sell it via LiveRamp's data marketplace, French data providers are limited to 30 million records and UK data providers are limited to 100 million records per file.[312]

Selling data via LiveRamp and other data marketplaces. "Data sellers" or "data providers" can sell segments either directly via LiveRamp's platform or send them to "destination platforms that accept third-party segments" and thus sell it via other data marketplaces.[313] In 2022, LiveRamp's UK website provided lists of "data marketplace destinations" available in France and the UK. This included data marketplaces operated by companies such as Oracle, Salesforce, Nielsen, Criteo, Quantcast, The Trade Desk, Pubmatic, Eyeota and Outbrain.[314] LiveRamp's docs state that data sellers can also sell segments via Google, Amazon and Microsoft's Xandr.[315]

Selling sensitive data via LiveRamp and Xandr. As recently reported, a spreadsheet file dated May 2021, which lists more than 650,000 segments sold by hundreds of data brokers globally via Xandr's data marketplace, shows that LiveRamp's clients sold more than 82,000 segments via Xandr in 2021, including very sensitive data.[316] According to the file, LiveRamp's clients sold, for example, lists of digital identifiers referring to cancer sufferers, pregnant women, union members, muslims, jewish people, African Americans, poor people, payday loan prospects, online gamblers, unemployed individuals who were "seen at clinics/hospitals" or users of the LGBT dating app Grindr.[317] While most of these sensitive segments may be not available in Europe, LiveRamp's data marketplace certainly facilitates the sale of massive amounts of personal data also in Europe.

Data governance and contractual measures. LiveRamp states that segments "have to be reviewed and receive privacy and business approval before becoming live in the Data Marketplace. Most segments are reviewed and approved by LiveRamp within 1-2 business days".[318] As LiveRamp reviews and approves segments, it has certainly some control over what is being sold via its data marketplace. According to LiveRamp, "permitted use cases" for "data marketplace data" include "digital ad targeting", "audience extension" (i.e."lookalike modeling"), "campaign analytics", "tv targeting" and "measurement".[319] LiveRamp provides an extra "data marketplace data policy", which prohibits selling segments related to sexual orientation, pregnancy and any "sensitive personal data or special categories of personal data as defined by GDPR". Segments related to "cancer" or other "health conditions that cannot be treated with over-the-counter medication or lifestyle modification" can still be sold as "custom segments".[320]

3.1.2.2 Reliance on LiveRamp's identity graph systems

LiveRamp's third-party data marketplace relies on the company's identity graph services, from "onboarding" or otherwise ingesting the data to the "Connect" platform to distributing it to destination data companies and other "data marketplace" destinations. "Data marketplace segments" can be "based" on "offline" identifiers (such as name, postal addresses, email addresses and phone numbers) or "online" identifiers (such as cookie or mobile device IDs).[321] Distributing them to "destinations" involves the same steps as described in sections 2.2.5.3 and 3.1.1. LiveRamp states that "whether data sellers onboard data via PII, cookies, or mobile device IDs", its data marketplace "unlocks true people-based marketing through deterministic cross-device identity resolution and reach expansion".[322] To enable a "broader monetization" of their "data

[311] https://web.archive.org/web/20220703093145/https://liveramp.uk/partners/
[312] https://docs.liveramp.com/connect/en/getting-started-with-data-selling.html [13.9.2023]
[313] https://docs.liveramp.com/connect/en/selling-data-with-the-data-marketplace.html [13.9.2023]
[314] https://web.archive.org/web/20220703093145/https://liveramp.uk/partners/
[315] https://docs.liveramp.com/connect/en/syndicating-data-marketplace-segments-on-destination-platforms.html [13.9.2023]
[316] https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you
[317] Xandr spreadsheet file (30mb) on archive.org: https://web.archive.org/web/20230525225541mp_/https://xandr-be-prod.zoominsoftware.io/bundle/monetize_monetize-standard/page/attachments/data-marketplace-buyer-overview/data_marketplace_public_segments_pricing_05212021.xlsx [8.6.2023]
[318] https://docs.liveramp.com/connect/en/data-marketplace-segment-review-and-approval.html [13.9.2023]
[319] https://docs.liveramp.com/connect/en/data-marketplace-permitted-use-cases.html [13.9.2023]
[320] https://docs.liveramp.com/connect/en/liveramp-s-data-marketplace-data-policy.html [13.9.2023]
[321] https://docs.liveramp.com/connect/en/getting-started-with-data-selling.html [13.9.2023]
[322] https://docs.liveramp.com/connect/en/value-proposition-for-data-sellers.html [13.9.2023]

assets", clients can utilize the "RampID" system to "expand" their "seed audience with lookalike modeling" by "deterministically matching online or offline data to Audience Extension Partners".[323]

LiveRamp's identity graph enables and facilitates these personal data transmissions. Data providers could not transmit and sell the data without LiveRamp's massive efforts to maintain its identity graph and link the transmitted data to personal data processed by "destinations". According to a recent annual report filed to the SEC, LiveRamp "generate[s] revenue from the Data Marketplace primarily through revenue-sharing arrangements with data owners that are monetizing their data assets on our marketplace".[324] As such, LiveRamp directly benefits from its clients' data sales that rely on LiveRamp's identity graph.

3.1.2.3 Other data brokerage programs

LiveRamp provides two other programs that appear to be even more problematic than its standard data marketplace:

- LiveRamp's **"transaction signal program"** lets data providers sell "raw transaction, clickstream, or location data" rather than "segments". For example, they can sell "in-store and e-commerce CPG and retail transaction data" linked to personal identifiers including "PII", cookie IDs, device IDs or custom IDs.[325] It is not clear from the docs whether this is available in Europe.
- LiveRamp's **"offline data marketplace"**, which is available only in the US, allows data buyers to directly append attributes ("such as demographic and psychographic data") to customer records that contain "PII" or AbiliTec IDs.[326]

3.1.3 Measurement and attribution

LiveRamp has also integrations with "destinations" that allow clients to "attribute" purchases and other actions performed by consumers to the digital ads served to them by these destinations. This typically involves complex chains of data flows, which may include clients uploading purchase transaction records to LiveRamp, and also makes heavy use of LiveRamp's identity graph. LiveRamp has attribution integrations with Facebook, Google, Microsoft, Criteo, The Trade Desk and other companies.[327] Section 3.2.4 describes how advertisers can use RampIDs to join their own data with "Google's advertising data" for measurement purposes.

3.2 RampIDs as universal identifiers in the broader data and adtech industry

LiveRamp explains that it is "connecting data across thousands of enterprises, publishers, technology platforms, data owners, and agencies". The RampID system "facilitates these connections, as well as many ecosystem-wide data collaborations".[328] LiveRamp itself sees the RampID as a "universal identifier" and a "people-based ID" that "represents an individual".[329]

Sections 2.2.5 and 3.1 show that clients can use LiveRamp's identity graph systems and its "Connect" platform to "connect" customer data and other consumer records, including about website visitors and mobile app users, to hundreds of adtech firms, data brokers, marketing intermediaries, platforms and publishers, some of which match it to their own databases that contain personal data about millions or billions of people. Clients can use it for digital profiling and ad targeting across the digital world and to measure and monitor how people respond.[330] They can use it to personalize their websites, apps and customer communication[331] and to buy and sell "segments", i.e. lists of identifiers referring to people with certain characteristics, via LiveRamp's data marketplace and other data marketplaces.[332]

---

[323] https://docs.liveramp.com/connect/en/data-marketplace-audience-extension-with-lookalike-modeling.html [13.9.2023]
[324] https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm
[325] https://docs.liveramp.com/connect/en/transaction-signal-program.html [13.9.2023]
[326] https://docs.liveramp.com/connect/en/offline-data-marketplace.html [13.9.2023]
[327] https://docs.liveramp.com/connect/en/attribution-programs.html [13.9.2023]
[328] https://liveramp.com/blog/identitylink-now-rampid/ [5.9.2023]
[329] See secton 2.2
[330] See section 2.5
[331] Ibid.
[332] See section 3.1.2

3.2.1 "Vendor-specific" RampIDs?

LiveRamp often emphasizes that RampIDs are vendor-specific. For every one of LiveRamp's clients or partners, a RampID referring to the same person looks different.[333] As such, it cannot be used as a single "universal" identifier across the ecosystem. While this is true in theory, the fact that RampIDs are vendor-specific may not matter much for two reasons. First, LiveRamp's clients and partners are often major players and data intermediaries who process personal data about millions of people "on behalf" of many other companies – all of whom will utilize RampIDs generated for the same intermediary. Second, LiveRamp provides "transcoding" services to convert and translate RampIDs specific to one vendor to RampIDs specific to another vendor.

Vendor-specific RampIDs are used by large players. According to a recent annual report filed to the SEC, LiveRamp has 825 direct clients globally and serves "thousands of additional customers indirectly" through its "partner and reseller network".[334] LiveRamp's clients and partners are typically larger players in the data and adtech industry, who themselves process personal data "on behalf" of myriad web and app publishers, advertisers and other businesses. The following excerpt from LiveRamp's docs[335] shows two vendor-specific RampIDs processed by Criteo and The Trade Desk (TTD), both of which are adtech firms who work with numerous advertisers and process personal data on hundreds of millions of people:

JSON


```
{
  "ttd": "Xi3022CxsryScO961hgy7Wv7z6H8fO4UZAEoUokyBg2wxLgt6TGleZlntpNJM_XUoYsebx",
  "criteo": "Xi1350AKEhNPrm_y49wWV0hW49_erVLMFKES7OgcEg5CoWzibxYiTdpzLQWWqvt_dUIjrI"
}
```


Figure 23 © LiveRamp

The above code fragment shows two "derived" RampIDs. As section 2.2.3 describes, "derived" RampIDs start with the characters "Xi". Both RampIDs refer to the same person but are "encoded" for different LiveRamp partners. The RampID partner encoding for The Trade Desk (TTD) appears to be "3022" and the RampID partner encoding for Criteo "1350". This example comes from a page that explains how RampIDs can be transmitted via the RTB bidstream in digital advertising.[336]

Vendor-specific RampIDs are interoperable across vendors. LiveRamp provides several mechanisms to convert, translate or "transcode" RampIDs encoded for one vendor to RampIDs encoded for another vendor. While "RampIDs are unique per each LiveRamp client", LiveRamp's "identity translation solutions" allow clients to "translate identifiers from one identity space to another" in order to "build strategic data partnerships through data collaborations leveraging LiveRamp's RampIDs":[337]

- Companies can use the "transcoding" endpoint of the RampID API to convert RampIDs encoded for one company to RampIDs referring to the same persons encoded for another company. LiveRamp states that it validates "certain privacy restrictions" before granting a company access to the ability to transcode RampIDs (see also section 2.2.5.2).
- Companies can use the "File-Based Recognition Workflow" (see section 2.2.5.1) to send files that contain a large number of RampIDs encoded for one company and receive files that contain RampIDs referring to the same persons encoded for another company.[338]
- Companies can also use LiveRamp's transcoding functionality directly on cloud-based data integration platforms such as Google BigQuery, Amazon AWS Sagemaker and Snowflake.[339]

[333] See section 2.2.3
[334] https://www.sec.gov/Archives/edgar/data/733269/000073326921000017/ramp-20210331.htm
[335] https://sidecar.readme.io/docs/deal-id-implementation [13.9.2023]
[336] See e.g. https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
[337] https://docs.liveramp.com/identity/en/identity-translation.html [13.9.2023]
[338] https://docs.liveramp.com/identity/en/transcode-rampids-using-a-file-based-recognition-workflow.html [13.9.2023]
[339] https://docs.liveramp.com/identity/en/identity-translation.html [13.9.2023]

3.2.2 RampIDs in the RTB bidstream in digital advertising

The following code fragments from LiveRamp's docs[340] show how RampIDs can be transmitted via the real-time bidding (RTB)[341] bidstream:

Figure 24 © LiveRamp

The figure on the left shows how a maintained RampID is transmitted in an OpenRTB 3.0 bid request. As detailed in sections 2.2.2 and 2.2.3, the prefix "XY" indicates a "maintained" RampID. A maintained RampID is persistently tied to "offline" identifiers such as a name, postal address, email address and phone number, and thus refers to a person LiveRamp "fully recognizes". The figure on the right shows how a maintained RampID and another pseudonymous ID created by the data broker Epsilon are transmitted in an OpenRTB 2.5 bid request.

In 2022, LiveRamp told shareholders that "65+ SSPs were live or committed" to broadcast RampIDs to the RTB bidstream and "75+ DSPs were live or committed" to bid on RTB requests that include RampIDs. While the phrase "live or committed" is ambiguous, LiveRamp also stated that 60 billion ad impressions were linked to RampIDs on average per day.[342] This means that at least some SSPs that have thousands of publisher clients and data on billions send pseudonymous RampIDs into the RTB bidstream. At least some DSPs that have thousands of advertising clients and data on billions match their own data with RampIDs in the RTB bidstream, and **RampIDs are processed in the bidstream 60 billion times per day**.

Sincera, an industry platform that tracks the use of identifiers in digital advertising, shows that 36,333 out of 270,000 web publishers, which it considers as globally relevant, use RampIDs to track users or sell their profile via RTB (chart on the left, as of September 13, 2023). Around 70% of the times publishers sent a RampID to the RTB bidstream, it was picked up by an advertiser (chart on the right):[343]

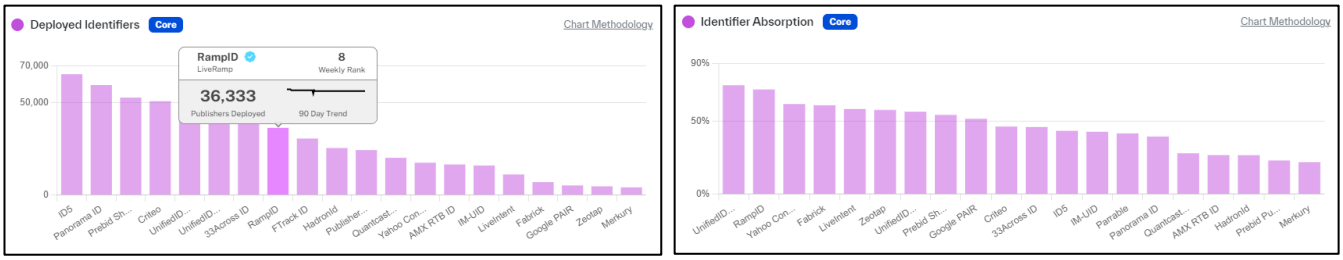


Figure 25 © Sincera

Adtech firms started to utilize the RampID, formerly known as "IdentityLink" (IDL),[344] in the RTB bidstream a few years ago. Some examples:

[340] https://sidecar.readme.io/docs/using-idls-in-openrtb [14.9.2023]
[341] See e.g. https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
[342] https://s29.q4cdn.com/969268860/files/doc_financials/2022/q4/RAMP-Q4'22-Earnings-Slides-FINAL.pdf [13.9.2023]
[343] https://app.sincera.io/ [13.9.2023]
[344] https://www.prnewswire.com/news-releases/liveramp-launches-identitylink-to-power-people-based-marketing-for-brands-300343299.html

- Criteo, the French adtech firm and DSP that mostly serves advertisers, announced back in 2019 that it "leverages" LiveRamp's "IdentityLink Bidding". By "bidding on IdentityLink", Criteo would create a "better consumer experience by linking both online and offline identifiers".[345]
- Rubicon Project,[346] an adtech firm and SSP that mostly serves publishers, also announced in 2019 that its "implementation of IdentityLink in the bidstream enables DSPs to directly transact on IdentityLinks (IDL)".[347]
- MediaMath, an adtech firm and DSP that mostly serves[348] advertisers, announced in 2020 that it will "natively bid, buy & attribute on LiveRamp IDL".[349]
- Index Exchange, an adtech firm and SSP that mostly serves publishers, announced in 2020 that it is "live and integrated with LiveRamp IdentityLink (IDL) globally". Publishers in Europe and the UK could now "infuse their supply with LiveRamp's pseudonymous, privacy-first, people-based identifier, IdentityLink", while advertisers could "recognize and transact" on the identifier.[350]
- The Trade Desk (TTD), an adtech firm and DSP that mostly serves advertisers, announced in 2022 that advertisers can already "buy on RampID […] within The Trade Desk's platform" and that it "plan[s] to enable bidding on RampID, LiveRamp's privacy-first, people-based identifier, within The Trade Desk in Europe".[351]
- Adobe "now supports RampID across channels, including desktop display, desktop video, mobile web, mobile in-app, connected TV (CTV), native, and audio", providing "people-based audience targeting, frequency capping, activation of first- and third-party data, delivery reporting, access to supply-side integrations and exposure logs, and measurement support", as announced by LiveRamp in 2022. The "integration is currently live in the United States, United Kingdom, France, Germany, Italy, Spain, Belgium, the Netherlands, Australia and Singapore".[352]
- The docs of the major adtech firm Xandr, a Microsoft subsidiary, describe how "third-party identity solutions" such as the "RampID" can be sent in RTB bid requests.[353]
- The "header bidding" technology Prebid[354] provides a RampID integration[355] for its "User ID Module".[356]

RampIDs often end up in the RTB bidstream via LiveRamp's "Authenticated Traffic Solution" (ATS) product, which includes another thin compliance layer called "identity envelopes", both of which are addressed in section 3.3.

RampIDs in the RTB bidstream and other profiling data. When RampIDs are transmitted in the RTB bidstream, they are typically linked to other personal attributes about the affected person, for example, to information about their browser and device, the website or mobile app currently in use, their real-time location and segment information, i.e. profiling categories (e.g. "this person loves dogs", "this person is interested in loans", "this person is a gambling enthusiast").[357] As such, vendor-specific RampIDs can be considered part of extensive personal data processing activities even if larger vendors would not use them "on behalf" of many other parties and even if RampIDs could not be "translated" across vendors.

3.2.3 LiveRamp's "identity coverage"

The previous sections shows that while RampIDs are formally vendor-specific, they can actually be used like universal identifiers, which is also how LiveRamp itself refers to them. RampIDs can serve as "join keys" across major data companies

[345] https://www.criteo.com/blog/criteo-liveramp-identitylink/ [26.6.2022]
[346] Now "Magnite": https://www.magnite.com/company/
[347] https://www.nasdaq.com/press-release/rubicon-project-announces-integration-with-liveramps-identitylink-2019-10-24 [14.9.2023]
[348] MediaMath went bankrupt in 2023: https://www.adexchanger.com/online-advertising/mediamath-files-for-bankruptcy-after-acquisition-talks-fall-apart/
[349] https://www.mediamath.com/blog/mediamath-becomes-first-dsp-to-natively-bid-buy-attribute-on-liveramp-idl/ [26.6.2022]
[350] https://www.indexexchange.com/2020/07/20/global-support-liveramp-identitylink/ [26.6.2022]
[351] https://www.thetradedesk.com/us/news/press-room/the-trade-desk-and-liveramp-to-lead-industry-effort-to-bring-new-privacy-first-interoperable-id-solution-to-meet-emerging-requirements-in-europe [14.9.2023]
[352] https://www.businesswire.com/news/home/20220223005423/en/LiveRamp-Collaborates-with-Adobe-to-Enable-Omnichannel-People-based-Targeting-and-Measurement [26.6.2022]
[353] https://docs.xandr.com/bundle/xandr-bidders/page/outgoing-bid-request-to-bidders.html [14.9.2023]
[354] https://docs.prebid.org/overview/intro.html [14.9.2023]
[355] https://docs.prebid.org/dev-docs/modules/userid-submodules/ramp.html [14.9.2023]
[356] https://docs.prebid.org/dev-docs/modules/userId.html [14.9.2023]
[357] This is how real-time bidding (RTB) works. See e.g. https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

and myriad clients and business partners, who utilize them to process, link and exchange personal data about millions of people every day.

Real-time bidding (RTB) in digital advertising is not the only area where RampIDs help businesses recognize people and link personal data about them across many companies at scale. RampIDs generally allow businesses to link personal data on their customers and other consumers across the digital world, far beyond the channels and platforms they operate themselves.

The following chart from LiveRamp's Q2 FY22 earnings slides illustrates how the company sees its "identity coverage":[358]

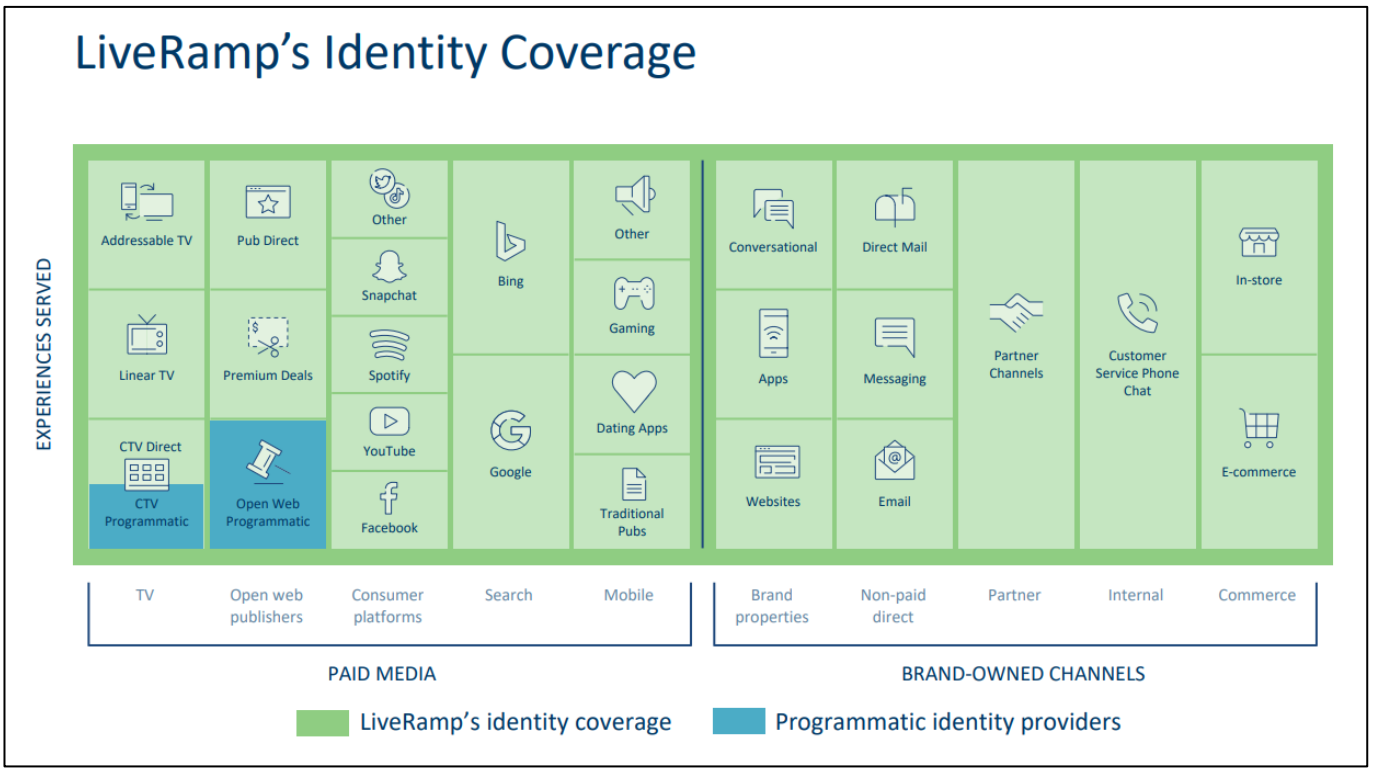


Figure 26 © LiveRamp

3.2.4 RampIDs as a "join key" between Google's data and its advertisers' data

Google explains that "RampID matching" enables its advertising clients to "leverage RampIDs as a join key between [their] advertising data and Google's advertising data".

For this purpose, "Google and LiveRamp build a match table, which associates LiveRamp RampIDs with Google IDs. This match table is used to translate between Google and LiveRamp's ID spaces". As a result, advertisers can match "hashed LiveRamp RampIDs with Google campaign data". While Google states that "joining" data via RampIDs "can provide a greater accuracy and a higher match rate than conventional cookie-based matching", it also emphasizes that the matching process still "depends on the use of cookies".[359]

This product is in "beta" and part of Google's "Ads Data Hub" system, which the company refers to as a "privacy-centric data warehouse" that is "the only access point" for Google's rich behavioral data sets that include "Google IDs", "mobile device IDs" and "user ids from publishers for measurement". RampID matching is restricted to "measurement" purposes. Google will match RampIDs to its own identifiers when users have interacted with ads served by Google or other vendors and "have a corresponding RampID". Google explains that "LiveRamp manages the majority of the implementation process" for this product, which also requires advertisers to enable LiveRamp's "file-based recognition" (see section 2.2.5.1).[360]

[358] https://static.seekingalpha.com/uploads/sa_presentations/938/75938/original.pdf
[359] https://developers.google.com/ads-data-hub/guides/liveramp-matching?hl=en [14.9.2023]
[360] Ibid.

3.3 LiveRamp's „Authenticated Traffic Solution" (ATS)

Announced by LiveRamp in 2019,[361] "Authentication Traffic Solution" (ATS) is one of several products offered by different vendors that promises to preserve web publishers' ability to sell behavioral advertising in times of increasingly restricted access to third-party cookies in the web browser.

Instead of cookie IDs, or sometimes in addition to them, **ATS creates a RampID based on the email address of website visitors** who registered at a site or otherwise disclose their email address to the website operator. This RampID can then be used as a pseudonymous identifier across the digital world. Initially, ATS creates an encrypted version of the RampID, a so-called "identity envelope", which is later decrypted in order to send a standard RampID via the RTB bidstream or to otherwise utilize it to recognize individuals, link other identifiers and personal data about them and act on them. ATS is also available for mobile app publishers. The RampID created by ATS can also be based on a phone number or other "offline" information.

As of 2022, 1,500 publishers have implemented ATS across 11,500 domains, including 80% of the "top 20" publishers and 78% of the "top 50" publishers, according to LiveRamp.[362] In 2021, this included, for example, the German Burda Media group, the French Prisma Media and "Microsoft Advertising, the world's second-largest publisher".[363] The ATS system is integrated with other adtech firms and intermediaries such as Pubmatic[364], OpenX[365] and The Trade Desk.[366] It is also, for example, integrated with "Amazon Publisher Services" where "tens of thousands of publishers" can activate it "in a no-code environment with a few simple clicks", as announced in 2022.[367]

As the next sections show, ATS relies on LiveRamp's identity graph systems. Because it uses "offline" information such as email addresses to create RampIDs, it specifically relies on LiveRamp's AbiliTec data.

3.3.1 Turning email addresses into personal identifiers for digital advertising

According to LiveRamp, ATS provides an "encrypted, persistent, people-based identifier throughout the programmatic supply chain, starting at the inventory source" to improve "programmatic addressability across the open web".[368] ATS "allows publishers to resolve consented user data with a RampID in real-time, enabling people-based advertising". Publishers can offer their "addressable RampID inventory for programmatic targeting".[369]

Put differently, ATS creates pseudonymous RampID identifiers that enables many different actors "across the open web" and "throughout the programmatic supply chain" to know that they are "talking" about the same persons. From its creation at the "inventory source", i.e. on a publisher's website, this identifier runs through chains of sophisticated encryption, decryption and translation operations, but in the end many different parties can make use of it.

The following chart from LiveRamp's docs describes how publishers can use ATS to "identify consumers" and then "transact" on RampIDs by transmitting them via the RTB bidstream[370] while "maintaining a consistent identity across platforms":[371]

[361] https://www.businesswire.com/news/home/20190530005338/en/LiveRamp-Launches-Authenticated-Traffic-Solution-to-Democratize-People-based-Identity-Across-the-Open-Ecosystem [14.9.2023]
[362] https://s29.q4cdn.com/969268860/files/doc_financials/2023/q2/RAMP-Q2'23-Earnings-Slides-FINAL.pdf [14.9.2023]
[363] https://liveramp.com/blog/liveramps-ats-drives-over-340-percent-roi-for-marketers-adoption-soaring/ [15.9.2023]
[364] https://pubmatic.com/news/pubmatic-establishes-global-integration-with-liveramp-on-identity-hub/ [15.9.2023]
[365] https://www.openx.com/press-releases/liveramp-taps-openx-as-authenticated-traffic-solution-ats-exchange-partner/ [15.9.2023]
[366] https://liveramp.com/blog/liveramp-enhances-authenticated-identity-infrastructure-support-unified-id-2-0/ [15.9.2023]
[367] https://liveramp.com/blog/liveramp-announces-integration-of-authenticated-traffic-solution-ats-into-amazon-publisher-services-aps/ [15.9.2023]
[368] https://developers.liveramp.com/authenticatedtraffic-api [14.9.2023]
[369] https://docs.liveramp.com/privacy-manager/en/authenticated-traffic-solution.html [14.9.2023]
[370] For real-time bidding (RTB) in digital advertising see e.g.: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/
[371] https://developers.liveramp.com/authenticatedtraffic-api/docs/the-basics [14.9.2023]

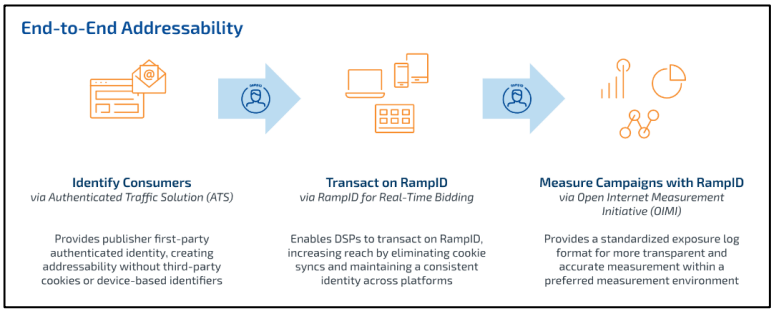
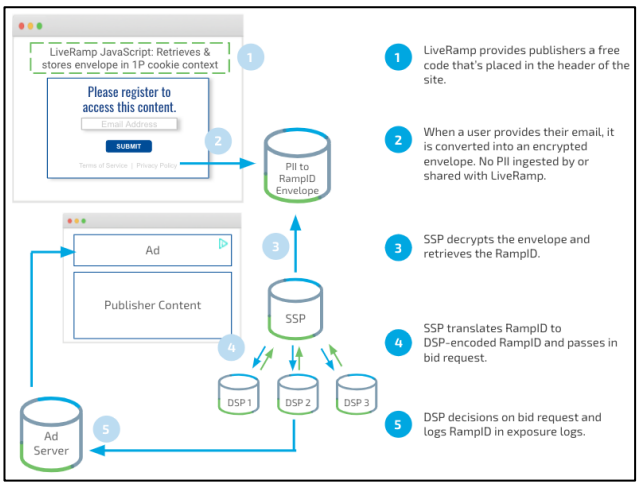


Figure 27 © LiveRamp

How a web publisher can use ATS. Typically, a website passes the email address of a site visitor to a Javascript tag, which is provided by LiveRamp and embedded into the site.[372] The website provider can obtain the email address, for example, because the user registered at the site or submitted a newsletter signup form. LiveRamp's Javascript tag can also automatically scan the website in the browser and detect, for example, an email address entered by the user.[373] The email address is sent to LiveRamp either in plaintext or in hashed format. LiveRamp then applies the usual RampID resolution process (see section 2.2). When it can "fully recognize" the person based on the provided email address, it generates a "maintained" RampID for the person. Otherwise it generates a "derived" RampID.

LiveRamp then returns an encrypted version of the generated RampID to the browser, a so-called "identity envelope". These identity envelopes look different for every publisher even if they refer to the same person.[374] The web publisher then stores the identity envelope for the recognized person in a first-party cookie or in the browser's local storage. Subsequently, the website can send the identity envelope to third parties[375], for example, to a "supply side platform" (SSP), which is an adtech firm that help publishers sell ad placements. As the identity envelope is stored in the user's browser, the website can retrieve it during subsequent visits to the site at a later point in time and again send it to third parties such as an SSP. LiveRamp's Javascript tag and its ATS functionality can organize and facilitate most of the process.[376]

The charts below from LiveRamp's docs describe a typical ATS implementation for digital advertising on the web that aims to recognize website visitors and send RampIDs via the RTB bidstream to "demand side platforms" (DSPs), which help advertisers buy and target ads. The chart on the left[377] includes the initial steps that occur on the publisher's website in the browser. The chart on the right[378] describes in more detail the subsequent process, including the decryption of identity envelopes and the transmission of RampIDs in RTB bid requests.



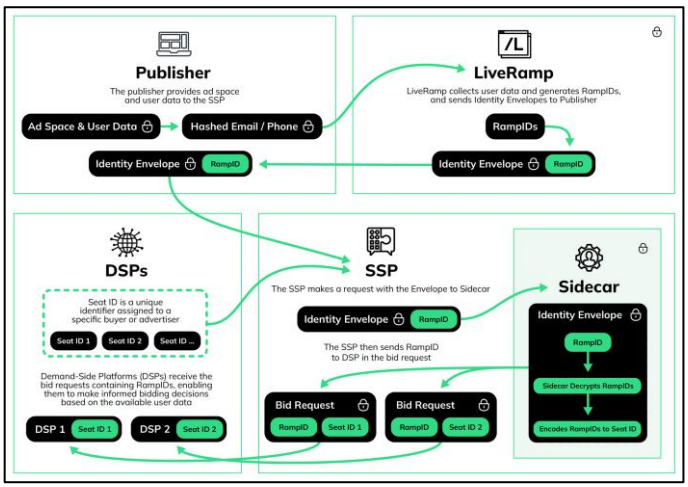


Figure 28 © LiveRamp

372 Ibid.
373 https://docs.liveramp.com/privacy-manager/en/configure-how-identifiers-are-obtained.html [14.9.2023]
374 https://docs.liveramp.com/privacy-manager/en/ats-security-and-pseudonymization.html [14.9.2023]
375 https://developers.liveramp.com/authenticatedtraffic-api/docs/6-return-stored-rampid-eenvelopes [14.9.2023]
376 https://docs.liveramp.com/privacy-manager/en/implement-ats-js.html [14.9.2023]
377 https://docs.liveramp.com/privacy-manager/en/authenticated-traffic-solution.html [14.9.2023]
378 https://sidecar.readme.io/docs [14.9.2023]

From "identity envelopes" to RampIDs in RTB. As shown in the chart on the right, ATS relies on publishers sending email addresses, phone numbers or other identifying information to LiveRamp, which returns encrypted versions of RampIDs it refers to as identity envelopes. These identity envelopes can then be sent from the websites (or mobile app) to a SSP company, which decrypts the identity envelope in order to retrieve the underlying RampID. For this purpose, the SSP uses a specific application provided by LiveRamp, which can be installed on the servers of the SSP and is referred to as "Sidecar".[379] To send the RampID from the SSP via an RTB bid request to one or several DSPs, which help advertisers respond to bid requests and buy targeted ad placements, the "Sidecar" application turns the RampID received from the website into DSP-specific versions of the RampID. Advertisers and DSPs can utilize these DSP-specific RampIDs for "identification purposes of the underlying browser in RTB bid requests" and "make informed bidding decisions based on the available user data".[380] As such, the entire ATS system only adds the concept of encrypted identity envelopes to the data practices already described in section 3.2.2. As soon as SSPs have decrypted the received identity envelopes, they can utilize the resulting RampIDs just as if encrypted identity envelopes had never existed in the first place.

LiveRamp's ATS system includes a wide range of functionality, especially when it is utilized for RTB, which cannot be examined in detail in this report. ATS can be deeply integrated[381] with the "header bidding" system Prebid[382] and its "User ID Module", which allows publishers to process and maintain several different pseudonymous identifiers for a person.[383] LiveRamp provides analytics technology for ATS[384] and mobile SDKs that can be embedded into iOS and Android apps.[385]

Processing third-party identifiers in identity envelopes? As described above, the Sidecar application can generate vendor-specific RampIDs from identity envelopes, which can then be transmitted via the RTB bidstream and matched to other personal data about the affected person by DSPs and other adtech intermediaries, who are able to "understand" those vendor-specific RampIDs. In addition, the Sidecar application can process identity envelopes that contain both RampIDs and other identifiers maintained by third-party data companies. LiveRamp states that "envelopes may contain more than one source of identifiers". This includes, for example, "UID2" identifiers maintained by the adtech firm The Trade Desk.[386] Sidecar "allows for the decryption of a single envelope" to "multiple available" identifiers.[387] In 2020, LiveRamp announced that its ATS system "will make" both "LiveRamp's identifier" and The Trade Desk's "UID2" identifier "available in the bidstream".[388] This functionality is not entirely clear and may be worth a further investigation.

3.3.2 Generating "identity envelopes", decrypting them and linking them to other identifiers

LiveRamp's identity envelopes contain RampIDs that are encrypted with "AES/CTR 128".[389] They are only "valid" 30 days from the date of their creation.[390] Publishers can, however, "refresh" them by calling a specific API, which extends their validity for another 30 days. LiveRamp "highly" recommends refreshing them "every 30 minutes when a user enters a new page".[391] When generating a new encrypted identity envelope with the help of LiveRamp, the result looks different even for the same underlying AbiliTec/RampID data, which makes it almost impossible to "understand" the encrypted RampID without LiveRamp's help. LiveRamp holds the encryption keys.[392]

LiveRamp provides several ways to decrypt identity envelopes or otherwise utilize them for personal data processing:

---

[379] https://docs.liveramp.com/privacy-manager/en/authenticated-traffic-solution.html [14.9.2023]
[380] https://sidecar.readme.io/docs [14.9.2023]
[381] https://docs.liveramp.com/privacy-manager/en/configure-prebid-js-for-ats.html [14.9.2023]
[382] https://docs.prebid.org/overview/intro.html [14.9.2023]
[383] https://docs.prebid.org/dev-docs/modules/userId.html [14.9.2023]
[384] https://docs.liveramp.com/privacy-manager/en/ats-analytics.html [14.9.2023]
[385] https://docs.liveramp.com/privacy-manager/en/implement-ats-mobile-sdk.html [14.9.2023]
[386] https://sidecar.readme.io/docs/environment-setup [14.9.2023]
[387] https://sidecar.readme.io/docs/api-specification [14.9.2023]
[388] https://liveramp.com/blog/liveramp-enhances-authenticated-identity-infrastructure-support-unified-id-2-0/ [15.9.2023]
[389] https://docs.liveramp.com/privacy-manager/en/ats-security-and-pseudonymization.html [14.9.2023]
[390] https://developers.liveramp.com/rampid-api/docs/envelope-decryption-endpoint [7.9.2023]
[391] https://developers.liveramp.com/authenticatedtraffic-api/docs/7-implement-the-ats-refresh-envelope-api [14.9.2023]
[392] Ibid.

- To decrypt "identity envelopes to RampIDs" for the "use by buyers downstream", SSPs and other adtech intermediaries can use "Sidecar", a "containerized Docker application" which receives decryption keys from LiveRamp.[393]
- The Sidecar application is, however, not the only way to decrypt identity envelopes. LiveRamp's "RampID API" provides an "identity envelope decryption endpoint" that can also be used to retrieve the underlying RampID.[394]
- While publishers can generally not link identity envelopes to other personal data before the decryption process, they can use LiveRamp's "Enhanced Client-Side Tag" (eCST) to track users based on picking up identity envelopes from the web browser and then record "segment" data in the "Connect" platform.[395] As such, publishers can utilize identity envelopes to create behavioral profiles.
- LiveRamp's "ATS API" provides an endpoint, which is labeled "beta" and promises to "retrieve matching segments for any given envelope".[396]

ATS and the "identity envelope" system can be used to send data to Facebook and Google:

- LiveRamp's "ATS Facebook CAPI Adapter" can generate "Facebook-scoped envelopes" in order to send "Facebook-encoded" RampIDs to Facebook's "Conversion API",[397] which allows advertisers to send "marketing data (such as website events, app events and offline conversions)" to Meta, for example, to "optimize ad targeting".[398] This requires Facebook to map Facebook-encoded RampIDs to its users, which may be facilitated via the Meta pixel.[399]
- Google's "Secure Signals" system, previously known as "Encrypted Signals", allows publishers to "share" LiveRamp's identity envelopes "directly with bidders that the publishers choose to work with". For this purpose, Google receives identity envelopes, which are then "included in RTB bid requests within Google's ad exchange". Google emphasizes that the "composition of the signals shared" is "controlled by the publisher, who also controls the list of eligible bidders". Identity envelopes "will only be shared at the publisher's explicit instruction and only with bidders the publisher has allowed to receive the envelope".[400] Despite all the disclaimers, identity envelopes are processed via Google's infrastructure in a way that allows advertisers to utilize identity and other data provided by publishers.
- Another system provided by Google, which it refers to as "Publisher Advertiser Identity Reconciliation" (PAIR), integrates ATS with Google's "Display & Video 360" system. For this purpose, ATS can return both identity envelopes and Google "Pair" IDs, which can then be passed "downstream to bidders by including the "Google PAIR ID module" in the Prebid configuration.[401] The system aims to "facilitate a secure and privacy-focused way for enabling advertisers and publishers to match their first-party data".[402] Put differently, advertisers can make use of personal data provided by publishers based on identity matching via LiveRamp and Google.

Identity envelopes can be generated from different types of personal data:

- LiveRamp's docs suggest that identity envelopes can not only be generated from email addresses and other "offline" identifiers, but also from cookie IDs stored in third-party browser cookies. The "ATS API" provides an endpoint that retrieves identity envelopes "using the LiveRamp third-party cookie footprint".[403]
- LiveRamp provides SSPs and other adtech intermediaries with "three primary methods to map cookieable traffic to Envelopes" on the web. They can call a "traditional cookie sync endpoint", which "will then redirect the traffic back with an identity Envelope - if available". LiveRamp also offers "mapping files to relate identity Envelopes to a cookie space", which appear to return identity envelopes mapped to cookie IDs, according to an example shown in the docs.[404] LiveRamp

[393] Ibid.
[394] https://developers.liveramp.com/rampid-api/docs/envelope-decryption-endpoint [7.9.2023]
[395] https://docs.liveramp.com/identity/en/implement-the-enhanced-client-side-tag.html [15.9.2023]
[396] https://developers.liveramp.com/authenticatedtraffic-api/reference/retrieve-segments-with-ats-envelope [15.9.2023]
[397] https://developers.liveramp.com/authenticatedtraffic-api/docs/facebook-capi-adapter [15.9.2023],
[398] https://developers.facebook.com/docs/marketing-api/conversions-api/ [15.9.2023]
[399] https://docs.liveramp.com/privacy-manager/en/facebook-capi-adapter.html [15.9.2023]
[400] https://docs.liveramp.com/privacy-manager/en/google-encrypted-signals-for-publisher-html.html [15.9.2023]
[401] https://docs.liveramp.com/privacy-manager/en/google-pair-and-ats.html [15.9.2023]
[402] https://developers.liveramp.com/authenticatedtraffic-api/docs/google-pair [15.9.2023]
[403] https://developers.liveramp.com/authenticatedtraffic-api/reference/retrieving-envelopes-cookieable [15.9.2023]
[404] https://sidecar.readme.io/docs/obtaining-identity-envelopes [15.9.2023]

also provides mapping files that link identity envelopes to mobile device IDs (Apple IDFA, Google AAID).[405] These mapping files are further described in section 2.2.5.5.

The above findings show that "encrypted" identity envelopes can be converted into RampIDs or linked to other identifiers in many ways. In a document submitted to the Californian privacy regulator, LiveRamp explains that an "identity envelope may be used instead of a cookie. It functions similarly in that it is a string of numbers and letters that represent your identity to various partners we work with".[406] The encryption may still be considered a technical measure that prevents some forms of unauthorized access. The system provides, however, many ways for "authorized" access, which entirely relies on organizational measures implemented by LiveRamp.

3.3.3 ATS as a thin compliance layer over the RampID system

Publishers and other parties who want to use the ATS system need a subscription and must pass a "privacy and data ethics" review carried out by LiveRamp. EU and UK publishers must implement a "consent management platform" that adheres to the IAB's TCF 2.0 system and list LiveRamp as a TCF vendor with the "purposes 1 to 10, special purposes 1 and 2, and features 1 and 2".[407]

Sample ATS privacy policies. LiveRamp provides sample paragraphs to be included in the privacy policies of ATS clients in different countries, including for the UK, France, Germany, Netherlands, Belgium, Italy, Spain, Romania and Poland. The UK sample paragraph tells users that LiveRamp will "create an online identification code for the purpose of recognising you on your devices" when they enter an email address on the client's website or app. This code "may be shared" with the client's "advertising partners and other third party advertising companies globally for the purpose of enabling interest-based content or targeted advertising".[408] This is quite explicit but still does not mention that LiveRamp matches the provided email address with data it maintains in its identity graph systems. The UK sample paragraph also states that this "code does not contain any of your identifiable personal data and will not be used by LiveRamp to re-identify" the user,[409] which are questionable claims.

Joint controllership for ATS. In the context of the ATS system, LiveRamp sees itself and other parties as "joint controllers" for certain personal data processing activities, according to terms for ATS clients like publishers/marketers[410] and SSPs[411] available on its website. According to these terms, LiveRamp and ATS clients "act as" joint controllers "in the Purpose of the Authenticated Traffic Solution ('ATS') and of LiveRamp Services Sidecar and RampID Envelopes". LiveRamp and SSPs "act as joint controllers "in the Purpose of LiveRamp Services Sidecar and RampID Envelopes". In both cases, the "distribution of responsibilities" is laid out in an extra document that describes the obligations of LiveRamp, ATS clients and SSPs.[412] In addition, LiveRamp provides terms for DMPs and DSPs, which do not address ATS.[413]

Conclusion. While ATS adds significant complexity to the RampID system and offers some benefits in terms of data security, it simply enables publishers and other clients to use email addresses and other "offline" identifiers as a means to link personal data across companies and connect the data to the broader adtech industry. Despite all the encryption, which is solely governed and controlled by LiveRamp, identity envelopes can be linked to other digital identifiers in many ways. ATS may be considered a thin compliance layer over the RampID system, just as the RampID system may be considered a thin compliance layer over LiveRamp's AbiliTec system. In the end, all the personal data processing and sharing that occurs in the context of the ATS system, including turning email addresses into RampIDs, creating identity envelopes and decrypting them, linking them

[405] Ibid.
[406] https://cppa.ca.gov/regulations/pdf/liveramp_sar_info.pdf [11.9.2023]
[407] https://docs.liveramp.com/privacy-manager/en/uk-and-eu-publisher-recommendations-for-liveramp-privacy-and-data-ethics-review.html [14.9.2023]
[408] https://docs.liveramp.com/privacy-manager/en/uk-and-eu-publisher-recommendations-for-liveramp-privacy-and-data-ethics-review.html [14.9.2023]
[409] Ibid.
[410] https://liveramp.com/authenticated-traffic-solution-country-specific-terms/ [14.9.2023]
[411] https://liveramp.com/privacy/ssp-country-specific-terms/ [14.9.2023]
[412] https://liveramp.com/distribution-of-roles-and-responsibilities-between-liveramp-and-the-publisher/ [15.9.2023]
[413] https://liveramp.com/privacy/dsp-dmp-country-specific-terms/ [15.9.2023]

to other identifiers and transmitting vendor-specific RampIDs via the RTB bidstream, relies on LiveRamp's identity graph systems.

3.4 Utilizing the identity graph via Google BigQuery, Amazon AWS and Snowflake

LiveRamp's identity graph systems are integrated with cloud environments from Google, Amazon and Snowflake.[414] As such, companies can "resolve and translate identifiers directly where the data lives". For example, they can "resolve[s] online device identifiers, including cookies, mobile device IDs, and CTV IDs, and hashed email addresses into a pseudonymous RampID" directly in the Amazon AWS cloud environment. [415] The websites of Amazon AWS and Snowflake state that this product is available for the US only.[416] Google does not make any statement about geographic restrictions.[417]

3.5 Additional LiveRamp products

LiveRamp provides several additional products and services. Two of them are briefly addressed in this section.

3.5.1 LiveRamp's "Safe Haven" product

In addition to LiveRamp's "Connect" platform, LiveRamp offers a product it refers to as "Safe Haven",[418] which promises to enable "data and audience collaboration in a neutral, permission-controlled, privacy-first environment to ensure the safety and security of data while delivering the highest possible matches between partners".[419] It appears to mirror much of the functionality provided by the "Connect" platform and also utilizes LiveRamp's identity graph systems,[420] but focuses on the exchange of personal data between two companies. Clients can still "combine" their data with "partner data" to "create and amplify audiences for targeting and personalization".[421]

3.5.2 LiveRamp's "consent management" and "tag management" services

LiveRamp offers a "consent management platform" (CMP), which it acquired in 2019[422] and which it refers to as "Privacy Manager".[423] Clients can optionally use it "for all third-party tracking technologies on all of [their] websites and mobile applications".[424] In addition, LiveRamp offers tools that help clients to implement LiveRamp's tracking and identity services:

- The "LaunchPad" service "acts as a single tag solution that streamlines workflow and simplifies the implementation of LiveRamp products".[425]
- The "tag management" service provides "consent on demand" and should make "the setup for hardcoded conditional firing as easy as never before".[426]

4. Concluding remarks

The findings of this technical report show that LiveRamp **maintains population-scale identity databases**, which tie different "offline" and "online" identifiers referring to a person to each other, including names, postal addresses, email addresses, phone numbers, device IDs, connected TV IDs, cookie IDs and "custom" IDs. In addition, these databases tie identity records the company considers to be part of a household to each other. LiveRamp maintains persistent "AbiliTec" and "RampID" identifiers referring to a large number of persons and households in its identity databases. It maintains comprehensive identity records

[414] https://docs.liveramp.com/identity/en/embedded-identity-in-cloud-environments.html [19.9.2023]
[415] Ibid.
[416] https://aws.amazon.com/marketplace/pp/prodview-v4557zxjo6ykq [19.9.2023], https://app.snowflake.com/marketplace/listing/GZT0Z11US77E/liveramp-retrieval-api-offline-to-online-identity-translation [19.9.2023]
[417] https://console.cloud.google.com/marketplace/product/mktplc-prod-liveramp-public/liveramp-gcp?project=mktplc-prod-liveramp-public [19.9.2023]
[418] https://docs.liveramp.com/safe-haven/ [19.9.2023]
[419] https://www.businesswire.com/news/home/20200302005147/en/LiveRamp-Launches-Safe-Haven-to-Enable-Data-Partnerships [19.9.2023]
[420] Ibid.
[421] https://docs.liveramp.com/safe-haven/en/understanding-safe-haven.html [19.9.2023]
[422] https://liveramp.com/blog/liveramp-acquires-faktor/ [19.9.2023]
[423] https://docs.liveramp.com/privacy-manager/en/privacy-manager.html [19.9.2023]
[424] Ibid.
[425] https://docs.liveramp.com/privacy-manager/en/launchpad.html [19.9.2023]
[426] https://docs.liveramp.com/privacy-manager/en/tag-management.html [19.9.2023]

about whole populations. In order to create its identity databases and constantly keep them updated, it obtains and purchases identity data from "offline" data providers, "match partners" and other third-party companies. LiveRamp performs these personal data processing activities in several countries including the UK and France. This raises the question of whether LiveRamp has a legal basis to maintain its identity databases under the GDPR. It also raises the question of whether LiveRamp has a legal basis to obtain the data from its identity data providers.

LiveRamp **utilizes its identity databases to help clients and other companies** link and match personal data about their customers, website visitors, app users and other consumers to pseudonymous RampIDs and other digital identifiers in order to combine personal data across different sources and databases, use it for digital profiling and personalization, and transmit the data to third-party companies such as adtech firms and large platforms for ad targeting and other purposes. Transmitting or "distributing" personal data such as "segments" to third-party companies also relies on linking and matching pseudonymous RampIDs and other digital identifiers maintained by LiveRamp to identifiers processed by these third-party data companies. Furthermore, LiveRamp utilizes its identity databases to help clients and other organizations buy personal data about consumers from other companies who sell personal data via its "data marketplace", which once again relies on linking and matching pseudonymous RampIDs and other digital identifiers maintained by LiveRamp to identifiers processed by data buyers and sellers. LiveRamp also utilizes its identity databases to help clients and other companies monitor activities of consumers who were exposed to digital ads, which also relies on linking and matching pseudonymous RampIDs and other digital identifiers maintained by LiveRamp to identifiers processed by clients and other companies.

These personal data processing activities, from combining and buying data to distributing and selling it, rely on linking and matching identifiers across databases, clients and other companies, and as such, on LiveRamp's identity databases. Many of these processing activities involve LiveRamp transmitting identifiers to other companies and LiveRamp receiving identifiers from other companies. When clients and other companies query LiveRamp's identity databases, for example, by sending consumer records that contain identifying information to LiveRamp in order to receive pseudonymous RampIDs, LiveRamp always tries to match and link the data to full identity records referring to persons or households. It tries to recognize and identify persons based on its identity databases and provides many other companies with the ability to recognize and identify people as well. Many of these processing activities, from combining and buying data to distributing and selling it, are facilitated by LiveRamp's cloud-based software systems, tags, APIs, third-party integrations and other mechanisms.

LiveRamp performs these processing activities in several countries including in the UK and France. This raises the question of whether LiveRamp has a legal basis to link and match pseudonymous RampIDs and other digital identifiers maintained in LiveRamp's identity databases to identifiers processed by its clients and other companies. It also raises the question of whether, or to what extent, LiveRamp determines the means and purposes for its linking and matching of pseudonymous RampIDs and other digital identifiers maintained in its identity databases to identifiers processed by clients and other companies. More broadly, it raises the question of whether, or to what extent, LiveRamp may determine the means and purposes for other personal data processing activities that rely on the linking and matching of identifiers across companies, from combining and buying data to distributing and selling it.

Pseudonymous RampIDs, which are provided by LiveRamp and refer to full or partial person records in its identity databases are **processed across many parties at an extreme scale**. Clients can use RampIDs and other identifiers provided by LiveRamp to combine information from entire customer databases that contain millions of consumer records with records from other sources. Clients can transmit or "distribute" these records to third-party companies, who use RampIDs and other identifiers provided by LiveRamp to link and match them to billions of consumer records processed by these third-party companies. Some third-party companies transmit RampIDs provided by LiveRamp via the RTB bidstream in digital advertising in order to link and match them to RampIDs processed by other third-party companies. So-called SSPs, which are adtech firms that operate on behalf of several or many publishers, create "bid requests" that contain personal attributes and RampIDs that refer to person records in LiveRamp's identity databases and transmit them to so-called DSPs, which are adtech firms that operate on behalf of several or many advertisers. DSPs receive personal attributes linked to RampIDs and can link and match them to their "own"

RampIDs also provided by LiveRamp. RampIDs are processed and transmitted in the RTB bidstream 60 billion times a day, according to LiveRamp.[427]

The data practices documented in this report suggest that RampIDs and other identifiers that rely on LiveRamp's identity databases play a major role in today's marketing surveillance ecosystem. They facilitate the exchange of personal data about consumers between thousands of publishers, advertisers, adtech firms, data brokers and large platforms. They allow businesses to link and combine personal data about their customers and other consumers to other personal data across the digital world, far beyond the channels, websites, apps or platforms these companies operate themselves. LiveRamp itself explains that it is "connecting data across thousands of enterprises, publishers, technology platforms, data owners, and agencies".[428] The RampID system "facilitates these connections, as well as many ecosystem-wide data collaborations". LiveRamp considers the RampID to be a "universal identifier" and a "people-based ID" that "represents an individual".[429] Google explains that "RampID matching" enables its advertising clients to "leverage RampIDs" as a "join key" between its client's "advertising data" and Google's "advertising data".[430]

Track, monitor, profile, target and single out persons based on "one way" pseudonymization. The basic idea behind LiveRamp's identity graph systems relies on a form of pseudonymization that is claimed to be "one way". Companies constantly send all kinds of identifiers to LiveRamp, including names, postal addresses, email addresses, phone numbers and a variety of digital identifiers. LiveRamp returns pseudonymous RampIDs that refer to partial or full person records in its identity databases. Companies rarely get access to the "original" identifiers they send to LiveRamp, but can use the returned pseudonymous RampIDs to link and match records. LiveRamp provides other companies with the ability to consistently convert personal data about consumers and their behaviors into personal data that is linked to pseudonymous RampIDs. Subsequently, they can match and combine records linked to RampIDs with records in other databases or processed by other companies that are also linked to RampIDs. This is a powerful concept, which enables many companies to track, follow and interact with data subjects across the digital world in many life contexts. As long as these companies use the same method to retrieve pseudonymous identifiers referring to the affected data subjects, they can use these pseudonymous identifiers to join personal data across databases and companies. This is what pseudonymous RampIDs facilitate. As such, LiveRamp's "one way" pseudonymization is hardly a measure that protects data subjects from re-identification and personal data linkage across contexts. Actually, RampIDs provide a more powerful way to join personal data across databases and companies than names. While RampIDs are pseudonymous identifiers which can be retrieved based on data collected in many contexts, they refer to comprehensive identity records about the affected data subjects.

RampIDs as "vendor-specific" or "universal" identifiers? While LiveRamp itself refers to the RampID as a "universal identifier", it also emphasizes that RampIDs are "vendor-specific". For each of LiveRamp's clients or partners a RampID referring to the same person looks different. This formally prevents RampIDs from being used as "universal identifiers". Only companies who understand RampIDs specific to a particular vendor can utilize them to exchange, link and match personal data between each other's databases. In practice, this may not however prevent RampIDs from being used as "universal identifiers" due to two reasons. First, LiveRamp has only a few hundred direct clients and partners, some of which are themselves intermediaries who process personal data about hundreds of millions of people on behalf of many clients themselves. As such, these clients can utilize vendor-specific RampIDs to exchange, link and match extensive personal data across many of their own clients. For example, adtech firms such as SSPs and DSPs process vendor-specific RampIDs on behalf of hundreds or thousands of publishers and advertisers. Second, LiveRamp provides functionality to convert RampIDs specific to one vendor to RampIDs specific to another vendor in order to help them "build strategic data partnerships through data collaborations leveraging LiveRamp's RampIDs".[431] LiveRamp has control over which companies are able to convert and link RampIDs specific to one vendor to RampIDs specific to another vendor.

Even if clients neither process data on behalf of many other firms nor convert vendor-specific RampIDs, LiveRamp's pseudonymous identifier can enable extensive data sharing, linking and matching across companies who process personal data

[427] See section 3.2.2
[428] See section 3.2
[429] Ibid.
[430] See section 3.2.4
[431] See section 3.2.1

about a large number of data subjects. A single data broker can, for example, utilize RampIDs to sell personal data about millions of people to several data buyers, who can then utilize RampIDs to transmit and distribute records to third-party companies which match these records to billions of consumer records they process themselves.

Despite the fact that RampIDs as pseudonymous identifiers represent a technical measure that may improve data security, RampIDs enable the exchange of personal data about millions of people across companies. Likewise, although the vendor-specific nature of RampIDs represents a technical measure that may improve data security, companies can use vendor-specific RampIDs to exchange personal data across many of their own clients or convert RampIDs specific to one company to RampIDs specific to another company. This raises questions about the organizational measures implemented by LiveRamp and about the true extent of personal data processing across companies facilitated by its identity databases.

Encrypted "identity envelopes". LiveRamp provides additional technology that makes it easier for companies to connect their customer data to the broader data and adtech ecosystem. Via the company's "Authenticated Traffic Solution" (ATS) product, publishers such as websites, mobile apps and other digital services can turn their users' email addresses or other "offline" identifiers into pseudonymous RampIDs, which can then be transmitted via the RTB bidstream in order to enable adtech firms and advertisers to profile and target these users while "maintaining a consistent identity across platforms".[432] Actually, these publishers do not receive or process RampIDs, but encrypted versions of RampIDs, which LiveRamp refers to as "identity envelopes". These identity envelopes are transmitted to adtech firms such as SSPs, who can decrypt them and retrieve the underlying RampIDs, which they can then transmit to DSPs via the RTB bidstream. Encrypted identity envelopes can be generated, decrypted and linked to other identifiers in different ways. Encrypting and decrypting identity envelopes is solely governed and controlled by LiveRamp. It entirely relies on potential or actual organizational measures implemented by LiveRamp. While encrypted identity envelopes add more complexity to the RampID system and offer some benefits in terms of data security, ATS can still be used to turn email addresses and other "offline" identifiers into pseudonymous RampIDs that can be utilized to exchange, link and match personal data across many parties.

A comprehensive compliance framework or house of cards? Each time a company utilizes a RampID to link and match personal data, it processes a pseudonymous identifier that is tied to a person's partial or full identity records maintained by LiveRamp. Without LiveRamp generating or providing the pseudonymous RampID, which relies on its comprehensive identity databases, the company could not perform this personal data processing activity. The findings of this report suggest that LiveRamp's ATS product and encrypted "identity envelopes" may be considered a thin compliance layer over the RampID system, just as the RampID system may be considered a thin compliance layer over LiveRamp's "offline" identity databases that contain names, postal addresses, email addresses and phone numbers. LiveRamp's identity surveillance technology and all the products and applications that rely on it are subject to a diverse range of data protection measures, including technical and organizational measures, as described in LiveRamp's software documentation and legal documents. The findings of this report, however, suggest that some of these measures are at least questionable. The findings suggest that LiveRamp's intrusive data practices may disproportionately affect the rights and freedoms of hundreds of millions of people in the UK, France and in other countries.

Data protection authorities in Europe and in the UK are the only entities, which could – and should – scrutinise the true nature and scale of LiveRamp's data practices, its role in the surveillance marketing ecosystem, technical and organizational measures implemented by the company and the lawfulness of its personal data processing activities under the GDPR and UK data protection legislation.

[432] See section 3.3.1