US Products Privacy Notice

Scope

Acxiom respects the privacy of every individual about whom we either process information or maintain information in our information products. This privacy policy describes our products and service offerings and the practices we follow to show that respect.

Acxiom has two primary lines of business. One is a broad line of information management services to help our clients manage their own customer and prospect information. Next, Acxiom offers a line of information products to augment the information our clients already have about their customers and prospects. Each is described in more detail below. Finally, our digital connectivity services assist our clients in connecting to third parties who can help them more effectively reach their audiences in the digital world, online, through mobile devices and other digitally enabled channels.

ACXIOM'S INFORMATION MANAGEMENT SERVICES

Acxiom's information management services provide end-to-end solutions to help our clients in the management, use, and optimization of their customer data and help them identify and reach potential new customers. These solutions can include marketing strategy services, advanced analytics to identify economic opportunity and lifecycle marketing improvements, new ways to connect with audiences, website experience optimization, and "big data' information management solutions. Our solution service infrastructure for clients can be hosted at Acxiom or at the client's location. When we provide information management services, we process our clients' and partners' information according to the terms and conditions of the contract.

ACXIOM'S INFORMATION PRODUCTS

Personal Information Collection and Use

Acxiom brings to market three types of information products, each containing only the information needed for the intended use. Each of Acxiom's information products is designed for specific use by our clients with a legitimate need for the product.

Marketing and Advertising Products: These products contain information on individuals and households in the U.S. and are developed from many sources, including:

- **Public record and publicly available information**: Telephone directories, website directories and listings, real property recorder, and assessor information.

- **Data from other information providers**: Demographic information, surveys, and questionnaires with appropriate notice and summarized or aggregated purchase information.

Acxiom's marketing and advertising products do not include specific details about a purchase, detailed financial information, credit information, medical information or Social Security Numbers. We will not knowingly collect, use, or disclose data for marketing purposes on anyone under the age of 18. We do use information related to children to identify and remove minor records from our and our clients' marketing files.

Acxiom also uses the U.S. Data & Marketing Association's (DMA) Mail, Telephone, and E-mail Preference suppression files, as well as state and federal do not call lists in the development of our marketing and advertising products.

Acxiom's marketing products are used by qualified companies, non-profit organizations and political organizations in their marketing, fundraising, customer service, and constituent service and outreach programs. The information can be used to enhance customer and constituent files and provide lists for prospecting and fundraising purposes. Acxiom's clients use our marketing and advertising products to provide customers and prospects with better service, improved offerings, and special promotions.

Acxiom enables our digital advertising clients and partners access to the Acxiom marketing data to deliver content that is relevant and meaningful to their users while respecting the privacy of consumers and offering them a choice about participating in such activities.

Directory Products: These products contain contact information such as name, address, and telephone number for most of the households and businesses in the United States. These databases are developed from the white and yellow pages of published U.S. telephone directories and information available through directory assistance.

Acxiom's directory products are used by companies, non-profit organizations, government agencies, political organizations, and consumers through internet sites to search the entire United States to locate names, addresses, and telephone numbers. For example, we license some of our directory products to companies as an automated and inexpensive form of directory assistance. We also license the directories to search engines on the internet that provide free nationwide directory searches to consumers.

Fraud Detection and Prevention Products: These products contain information about individuals and households in the United States for risk mitigation, including identity verification, information verification, fraud detection, and fraud prevention. We will not knowingly collect, use or disclose data for these purposes on anyone under the age of 13. These products include information from many different sources, such as:

- Directories, real property recorder and assessor information, current drivers' license information, where allowed by law, current motor vehicle information, where allowed by law, deceased information, and other suppression information.

- Data from other information providers: Telephone companies, surveys and questionnaires with appropriate notice, consumer-provided contact information and identifying information from credit bureaus where permitted by law.

These products and access to other information providers' services may include, where permitted by law, Social Security numbers and other information typically considered sensitive.

Acxiom's fraud detection and prevention products are used by qualified companies (primarily in the finance, insurance, mortgage, real estate, and retail industries), non-profit organizations and government agencies to verify the identity of consumers and to investigate suspicious transactions for fraud prevention. The basic verification service tells our client whether identifying information provided by a consumer is valid, current, and correlates to that individual. To protect the use of this information, Acxiom does not provide our fraud detection and prevention products to individuals.

Additional Terms and Conditions: For a company to use Acxiom's products and services, they are required to enter into a contract with Acxiom. The terms of these contracts may further govern the use of personal information collected and maintained by Acxiom.

Offshoring: Where permitted by law, third parties under contract to Acxiom may have access to the information in Acxiom's information products for the purpose of assisting in processing the data. Some of these third-party contractors may reside outside the United States.

Your Choices and How to Contact Us about our Information Products

Opt-Out from Acxiom's Marketing Products: Acxiom gives consumers the opportunity to opt-out of our marketing and directory products at no cost.

Acxiom utilizes the Data & Marketing Association's Mail, Telephone, and E-mail Preference files, as well as the various state registries and the Federal Trade Commission's Do-Not-Call Registry in developing our marketing and directory products.
Consumers registered with any of these organizations do not need to also opt-out with Acxiom to prevent use of information related to them for prospecting purposes. Consumers who wish to opt-out of all Acxiom marketing information products may complete and submit an opt-out request form by visiting https://www.acxiom.com/about-us/privacy/us-consumer-choices/. To learn about, view and edit, the information that determines the Acxiom-data-enabled ads you see offline or the digital offers you receive, please visit Acxiom's AboutTheData.com consumer website where we describe how data fuels marketing and helps you get the right offers at the right times.

Acxiom will also accept opt-outs from certain qualified third parties. To obtain a copy of Acxiom's third-party qualification criteria, please send an e-mail to privacy@acxiom.com.

Access and Correction to Acxiom's Directory and Fraud Detection and Prevention Products

Products: Acxiom offers access to, and correction of, information in our directory products and our fraud detection and prevention products.

Access to information about you in our directory and our fraud detection and prevention products will be provided in the form of a US Reference Information Report that is available for a processing fee of $5. You may complete and submit a request form for your US Reference Information Report by visiting https://www.acxiom.com/about-us/privacy/us-reference-info-report/. Alternatively, you may email us with questions at referencereport@acxiom.com or by calling 1-877-774-2094 toll free. After you receive your US Reference Information Report, you may contact us online, by phone or in writing about correcting any inaccurate information with Acxiom and with the original source of the information.

Complaint Process: Acxiom provides consumers a formal method for filing a complaint about our practices or procedures. This method specifies what information must be included in the complaint and where it should be directed. To learn how to file a complaint, e-mail us at privacy@acxiom.com or call 1-877-774-2094 toll free.

Other Questions: If you have any other question about any of Acxiom's information practices or products, email us at privacy@acxiom.com or call 1-877-774-2094 toll free.

ACXIOM'S DIGITAL CONNECTIVITY SERVICES

LiveRamp, an Acxiom company, provides Connectivity Services designed to enable our clients to reach consumers with greater efficiency and more relevant messages across various digital channels, including online, mobile, email, and addressable TV.

The purpose of this section of the Privacy Notice, is to help consumers, clients and partners understand how the LiveRamp connectivity services work, what data is involved in these services and what measures we take to respect the privacy of the data with which we have been entrusted.

LiveRamp Connectivity Services

The LiveRamp Connectivity Services include data onboarding, linking, and distribution to many of the players in the digital advertising industry to enable smarter targeting with more relevant messages and more accurate measurement. Onboarding is a service that loads data collected offline into the digital ecosystem, so it can be used for digital advertising purposes. The players include advertisers wishing to reach consumers, advertising supported websites, advertising supported apps, and addressable TV channels.

Today consumers interact with advertisers and brands through a variety of channels – offline and digital. This cross channel interaction is known as "omni channel." LiveRamp services are used to support these interactions for several types of entities in the digital advertising industry, including:

Marketing Platform Partners: LiveRamp has partnerships for distribution with hundreds of media and technology providers in the online, app and addressable TV ecosystem. With these partners, LiveRamp enables advertisersto display relevant ads to specific individuals through websites, mobile apps, and addressable TVs.

Third Party Data Providers: LiveRamp also offers services that allow third-party data providers, including Acxiom Information Products, to onboard their offline marketing data and sync their digital data in such a way that it can be used by advertisers to display more relevant ads to consumers.

Brands: LiveRamp offers connectivity services to digital marketers that advertise to consumers:
* Brands can onboard their proprietary offline and digital data for their own use to target advertising messages on their own website and/or their own mobile apps.
* Brands can use their own onboarded proprietary data along with third party onboarded data to offer more relevant ads through LiveRamp partners.
* Brands can also connect performance information about their omni-channel ad campaigns to understand how to improve the effectiveness of future campaigns. Performance information includes data about who viewed the ad, who clicked on the ad, as well as who actually responded in some way to theoffer.

Other Digital Partners: There are other players in the digital advertising industry that LiveRamp partners with to enable our Connectivity Services. These include cookie, mobile and addressable TV match partners that allow LiveRamp to recognize an individual across various channels. In addition, LiveRamp sells Connectivity Services to other third party advertising service providers to help facilitate their offerings.

Connectivity Services Work Across Channels

Due to technical differences across the channels, LiveRamp uses different approaches tailored specifically to each channel to provide our Connectivity Services. The common basis of these services is an ID that LiveRamp assigns to an individual. The ID may be used in a personally identifiable state or in an anonymous state, depending on the channel and the use.

LiveRamp collects certain types of information in connection with our Connectivity Services. This includes personal information such as name, postal address, email address, and phone number if permitted by our partners and clients through policy notices they have provided to consumers. We also collect non-personal information such as IP address, mobile device ID, and browser and operating system type and version. In addition, we handle, process, and share both

personal and non-personal information with our marketing platform partners in the course of performing our services; however we do not retain or use this information for our own internal business purposes unless permitted by our clients.

LiveRamp Cookie-based Connectivity Services:

Connectivity Services for cookie-based integrations are based on a LiveRamp ID and a LiveRamp cookie that together identify a browser. The cookie containing the ID is set when a consumer visits the website of one of our cookie match partners as a registered user, or when a consumer opens certain emails from a cookie match partner. Because match partners know the consumer, they enable LiveRamp to recognize the consumer as well and set the LiveRamp cookie containing the appropriate ID.

For example, our match partners may enable us to place or recognize a cookie on a consumer's computer or device, and our match partners may share personal information with us, such as your name, postal address, or email address. LiveRamp uses the personal information to link an ID to information stored in the browser or device. We may also collect information such as the device's IP address and the browser or operating system type and version. We use the combination of this information to recognize consumers across different channels and platforms over time for the purposes of facilitating online advertising, analytics, attribution, and reporting purposes.

For cookie-based integrations, three types of connections are maintained. The first is the connection between LiveRamp cookies and marketing platform partner cookies, a sync that enables LiveRamp to distribute advertising data to partners on behalf of our clients. In this case, the LiveRamp cookies containing LiveRamp IDs are synced with cookies set by our marketing platform partners.

The second connection is between LiveRamp cookies and third-party data providers. In this case, third party data providers onboard their data and LiveRamp matches it to the appropriate LiveRamp IDs, thereby connecting the data to the correct LiveRamp cookie.

Finally, the third connection is between a brand's data and the LiveRamp cookie. When marketers onboard their data, LiveRamp associates the brand's data with the LiveRamp ID, thus connecting this data to the LiveRamp cookies.

Once all these connections are made, a marketer can use them to understand how ad or email marketing campaigns perform and deliver ads or offline marketing to specific individuals when they visit a website with ad inventory. For example, we may facilitate the delivery of an ad to an individual in his or her web browser based on a purchase he or she made in a physical retail store, or we may enable a brand to send a personalized marketing email to that individual based on the fact that he or she visited a particular website.

LiveRamp cookies are set with an RLCDN.com name and expire after 180 days unless they are renewed or refreshed. Unlike web "tracking" cookies, LiveRamp cookies do not "track" users' behavior across websites. Instead, LiveRamp cookies are used only to recognize an individual so that relevant messages can be delivered to the intended recipient.

LiveRamp Mobile Connectivity Services:

Connectivity Services for mobile ID integrations are similar to cookie integrations except they use the mobile advertising ID assigned to the device instead of a cookie – namely the Apple ID for Advertising (IDFA) and the Android Advertising ID (AAID). We associate the LiveRamp ID with the mobile ID just like we would associate the cookie. LiveRamp links marketing platform partners, third party data providers, and data from a brand to mobile devices through the LiveRamp ID.

Mobile advertising IDs do not expire like cookies. Instead the device gives the user the ability to change the ID at any time, thus breaking the connection between the old ID and the device. Consistent with our online policy, LiveRamp IDs

are used to recognize individuals so relevant ads and offline marketing can be delivered and campaigns can be measured.

LiveRamp Addressable TV Connectivity Services:
Connectivity Services for addressable TV integrations are similar to online and mobile services except they use the subscriber ID assigned by the carrier to the set-top box instead of a cookie or a mobile ID. We associate the LiveRamp ID with the subscriber ID just like we would associate the cookie or mobile ID. LiveRamp links marketing platform partners, third party data providers, and data from a brand to subscriber IDs through the LiveRamp ID.

Addressable TV subscriber IDs do not expire like cookies. Instead the carrier gives the user the ability to determine if they wish to see targeted advertising on their TV. Consistent with our online and mobile policy, LiveRamp IDs are used only to recognize individuals so relevant ads can be delivered and campaigns can be measured.

Personally Identifiable versus Anonymous Connectivity:
LiveRamp may recognize an online, mobile or addressable TV user in two ways. First when our match partner shares personally identifiable information (PII) with us, or second when they share anonymized information with us, such as a hashed email address or an anonymous mobile ID. When they share PII, we can recognize a consumer on an identifiable basis. However, to preserve user privacy, we create an anonymous LiveRamp ID when we combine it with other anonymous data.

LiveRamp, like its Acxiom parent, values the preservation of consumer privacy, designing its systems and services to treat PII and other information that is not used to identify individuals with utmost care. LiveRamp chooses the appropriate LiveRamp ID, either PII or de-identified, based on the services it has been asked to perform; it does not mingle the two in any way that compromises user protections or choice.

Your Choices and How to Contact Us about LiveRamp Data Connectivity Services

Opting-Out of LiveRamp Connectivity Services

LiveRamp gives consumers the opportunity to opt-out of all our Connectivity Services. Click here to learn about permanent email-based opt-out features and to access our cookie-based opt-out. We also offer a mobile device ID opt-out here.

LiveRamp is a member of the Digital Advertising Alliance (DAA) and adheres to the DAA Principles for Online Behavioral Advertising and Multi-Site Data, as well as related guidance. LiveRamp subscribes to the DAA's industry-wide cookie opt-out mechanism that can be found here and its mobile device ID opt out available through its AppChoices app. Consumers who choose to opt out through these DAA mechanisms do not need to opt out of the equivalent mechanism with LiveRamp.

Keep in mind that opting out of LiveRamp through our opt-out channels or through the DAA does not disable advertisements altogether. Instead, opting out means that LiveRamp services will no longer be used to facilitate targeted advertising to your browser, device, or email address. In other words, you will still see advertisements, but they will be less relevant to you.

If you create a new email address, reset the mobile advertising ID on your device, or use a new browser, you will need to apply the appropriate opt out to that new email address, new device ID, and/or new browser as opt-outs are not necessarily transferred between email addresses, browsers, or devices.

Opting-Out with LiveRamp Partners

LiveRamp requires that our partners meet the same high standards we have. We contractually require that our match partners employ notice and choice mechanisms, and we work with other information service providers and our partners to assist them in following their respective industry standards.

How to Contact Us
If you wish to contact our privacy team about LiveRamp Connectivity Services, please send an email to privacy@acxiom.com or call 1-877-774-2094 toll free.

OTHER IMPORTANT INFORMATION

European Union Model Contracts: As a global company, Acxiom abides by privacy laws of many countries. Acxiom maintains an industry-recognized leadership role in consumer privacy and was one of the first U.S. companies to register with the U.S. Department of Commerce for EU Safe Harbor. In addition to being certified under its replacement, the EU-US Privacy Shield Framework, Acxiom has executed EU-approved model clauses with its EU subsidiaries to ensure ongoing compliance with the international transfer principle as set out in the EU's General Data Protection Regulation.

Accuracy: Acxiom maintains quality control procedures to ensure the information we compile and process is as accurate and complete as possible. Acxiom responds promptly to questions from clients and consumers about the accuracy of information.

Security: Acxiom maintains security procedures designed to keep information we own, license and process from being accessed by any unauthorized person or business. We use a variety of multi-level security systems to control access to our services and information products. All users at client locations, as well as all Acxiom associates, must have the appropriate access codes and be authorized to access certain data and applications.

Acxiom conducts risk assessments and regular audits on our internal and external information systems to assess our ability to maintain the integrity of client and Acxiom data. Our enterprise security operations center maintains real-time monitoring for information system vulnerabilities and unauthorized access attempts into our internal systems. We also maintain physical security for our facilities and limit access to certain critical areas of our business.

We take reasonable precautions to ensure that our security procedures are adequate for the protection of our computer systems and data, but this does not eliminate the possibility that our security will be breached. If a security breach causes Acxiom leadership to believe individual consumers are at actual risk for identity theft or other fraudulent activities that may cause substantial harm or inconvenience to consumers or if such breach otherwise requires public notification, Acxiom will post a security alert notice on our website (www.acxiom.com) that will provide relevant information for consumers and Acxiom clients to consider to protect against fraudulent and other harmful actions that may result from the unauthorized access.

Compliance: Acxiom participates in industry efforts to establish fair and workable guidelines above and beyond current laws and regulations and believes such actions are an effective way to protect privacy in the marketplace. We also support legislation and regulatory efforts to introduce fair and workable guidelines that protect privacy of consumers.

We actively work to ensure that such guidelines are consistent with, and complement established self-regulatory measures and that they enable the consumer to continue receiving the benefits that appropriate information use, sophisticated marketing techniques, and transaction-processing services provide.

When Acxiom provides information management services to our clients, we process our clients' information in strict accordance with the terms and conditions of the contract. Some of the services we provide to companies such as financial institutions and healthcare organizations are governed by laws such as the Fair Credit Reporting Act, Gramm-Leach-Bliley, the USA PATRIOT Act, and the Health Insurance Portability and Accountability Act. In these and similar situations, Acxiom works closely with our clients to ensure the processing we perform is in accordance with all the laws governing those activities.

Awareness: Acxiom is committed to privacy education. We provide education to our clients, our associates, and the industry about the issues, guidelines and laws surrounding individual consumer privacy issues, corresponding responsibilities and Acxiom's privacy policies and practices. Acxiom provides education and consultation to clients about privacy compliance and about the laws and industry guidelines that protect consumers. Acxiom advocates speak at various events and emphasize the importance of responsible data collection and use.

Privacy Policy Changes: From time to time Acxiom may update and revise our privacy policy based on changes in our business environment and changes to applicable law. We urge consumers and clients to periodically visit our website to understand any changes that may have occurred.

Our privacy policy contains an "effective date" reflecting when the last changes occurred.

Effective Date: May 25, 2018 .