

# RetailNext Privacy Policy

Effective date: 1 June 2016

This policy relates to the practices of RetailNext Inc. ("RetailNext") regarding our website and the products and services we sell.

This policy tells you how RetailNext handles the data of individuals ("you"). Our products are sold to companies. To understand how these companies handle your data, you should review their privacy policies to determine their practices.

## What We Do

RetailNext offers a set of products and services (the RetailNext "platform") used by retailers to analyze things that happen in and around their stores. Our customers may use our products and services to collect data from sensors, including video cameras, smartphone detectors, Wi-Fi networks, or other devices, to use along with other data, like purchases, loyalty program information, weather, and third-party information. We also provide ways to let our customers' shoppers opt into analytics and marketing programs, like through free Wi-Fi networks or mobile apps.

Our customers can choose to operate our platform entirely on their own, or they may choose to let us operate the software on their behalf as an online service. To understand what our customers do with the data they receive from us or collect directly, please consult their privacy policies directly.

When our customers request us to provide the service for them, we collect data on their behalf, and some of our customers elect to share some of that data with RetailNext so that we may use it to measure overall retail trends or to provide general demographic information about shoppers to our entire customer base. For example, we periodically issue reports on industry trends, like the report available at <http://retailnext.net/benchmark/>.

## What We Collect

Our platform supports the analysis of several different data sources. Our privacy policy focuses on the data that's generally gathered during a visit to a retail store, but each of our customers may use the platform in a different way and include data from many different sources. For example, our customers may correlate the data discussed in this policy with their own loyalty program data and point-of-sale transaction logs, third-party financial transaction data on purchasing history, or staffing data like the number of employees working during a given time period.

**Smartphone Location Detection.** RetailNext determines the location of a smartphone or wireless computing device by observing Wi-Fi or Bluetooth signals broadcast from that device. Individual devices are identified by a unique number (called a "MAC address") assigned to the

device when it was manufactured. RetailNext logs the MAC address of these broadcasts along with the time, the signal strength, and the location of the observing sensor. RetailNext does not store the payload of wireless network packets (meaning the data that end users are sending or receiving over a Wi-Fi or Bluetooth network). Unless you explicitly opt into a related service from one of our customers, it is our policy never to use this data to identify a person by name. It is used to measure things like store occupancy or the ratio of first-time to returning shoppers.

**Video Recording and Location Detection.** RetailNext analyzes data from video cameras to determine the paths people take through a physical space and to try to ascertain certain qualities about people, like age or gender. Our customers use this kind of information for marketing and strategic purposes, such as to improve the layout of their stores and offer the products that most interest their shoppers. For other examples, please visit our website at <http://retailnext.net/products/>. Video is usually available for playback by the customer in the RetailNext platform. In addition to analyzing traffic flow through a store or around a particular feature of a store, video is often used to investigate theft. Additional uses of video are determined by the customer.

**Guest Wi-Fi Internet Service.** When customers use our service to offer Wi-Fi Internet "hotspots" at their locations, registration is sometimes required. Registration data from these services is sent to us, but the exact nature of the information categories requested is determined by our customers when they create the user registration process. Some customers only require that users read and acknowledge the terms & conditions of use, but others may request personal information like name, telephone number, or email address. Information about the web browser used for registration, like the device type, operating system, and browser version, is collected automatically and sent to us and the customers.

We also collect information about use of the World Wide Web by observing outbound HTTP requests (non-secure web page requests), which may include web browser information, the URL (web address) of each page visited, search terms used, products viewed and saved on retail websites, and information entered into online forms. Information transmitted over secure connections (such as over HTTPS or a VPN) is not collected by us.

**Marketing Programs.** When customers use our service to automate some portions of their marketing programs, including websites, text messages, promotions on printed receipts, and other programs, some personal information may be shared with us to improve and measure the relevance of those offers to a consumer. This information may be linked to an identifier provided by a marketing program user (shopper), including email address, phone number, or loyalty program ID number. We may also use other information provided to us by a retailer.

## **Who We Share With**

Our customers have access to most of the data we collect on their behalf. Their use of the data is governed by their privacy policies and practices, and our customers may direct us to share data we collect with third-party service providers acting on their behalf. This can include

vendors who provide services for customer relationship management (CRM), marketing program management, business intelligence and analytics, workforce management, and loss prevention.

We also contract with third-party service providers, such as virtual hosting infrastructure providers, to host our servers and databases and to provide other services to us. It is our policy to request that our service providers agree not to access or use any information or data they may have access to while providing services to RetailNext other than as specified by us and for the purpose for which it was originally collected. Storage of this data is not always in your home country and may be transported across borders. As of the date of writing this, we store data in the United States, but we may add additional storage and processing sites without notice.

Through our platform and contractual agreements, it is our policy to place limits the use of smartphone location data if a user has not explicitly opted into a related service (like a free Wi-Fi network). Unless a user has opted in, it is our policy not to share the actual MAC address of a device except as described in the "Government Requests" section below. It is also our policy to require customers to agree not to use this data to attempt to identify people without their permission.

## **Security**

Once data is received by RetailNext's online service from our customers' sensors, it is our policy to encrypt it as it passes between our internal services, and to encrypt it when it is at rest. We take steps, like employing firewalls and two-factor authentication, to safeguard sensitive data and prevent unauthorized access to it.

When our customers operate our platform on their own, they are responsible for maintaining the security and privacy of the data.

## **Government Requests**

Notwithstanding anything to the contrary in this policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or rights of RetailNext or others. However, nothing in this policy is intended to limit any legal defenses or objections that you may have to a third-party or government request to disclose your information.

## **Data Retention**

In our hosted systems, customers may retain aggregated data indefinitely, but it is our policy to limit the retention of personal data to 2.5 years, and we allow customers to set a shorter limit. Retention of data that customers may export and store outside our hosted systems is governed by their privacy policies and practices.

## **Data Access, Correction, Deletion**

If you wish to access, correct, restrict, or delete data collected about you, you may submit a

request to the contact info below. Provided you have provided us with sufficient information to identify you and verify your identity, we will use reasonable efforts to comply with your request where legally required.

### **Opting Out of Some Data Collection**

You may opt out of some portions of the service, like Smartphone Location Detection and Guest Wi-Fi Internet Service analytics, by using our online form at <https://privacy.retailnext.net/> or by submitting a request to the contact info below.

When you opt out, we will take measures to delete historical data about your device and avoid collecting data about your device in the future.

### **Change of Control**

If RetailNext is involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your information may be sold or transferred as part of that transaction. The promises in this policy will apply to your information as transferred to the new entity, including your right to request to opt out of the service as described above.

### **U.S.-E.U. Data Processing**

Until a suitable replacement program like Privacy Shield is available, RetailNext continues to comply with the U.S.-E.U. Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement for data processed under that framework. To learn more about the Safe Harbor program and its status and to view our certification, please visit the U.S. Department of Commerce website at <http://export.gov/safeharbor/>.

We will investigate and attempt to resolve any complaints and disputes submitted to the contact info below. If a complaint or dispute cannot be resolved through our internal process, we agree to participate in the dispute resolution procedures of the American Arbitration Association (<http://www.adr.org>) pursuant to the Safe Harbor Principles.

### **Visiting our Websites**

We operate several websites, including those used for marketing, customer support, and opt-out choice. We use cookies (a small text file placed on your computer to identify your computer and browser) and/or web beacons (a file placed on a website that monitors usage) to measure usage and improve the experience of our websites. You can configure your web browser to refuse all cookies or to indicate when a cookie is being sent.

When you visit our websites, we use third-party services for hosting, analytics, advertising, customer support, content acceleration, and other promotional purposes, including Google (Analytics, Ad Services, Tag Manager, Hosted Libraries), Marketo, LeadLander, Crazy Egg, Disqus, Gaug.es, Salesforce, GetFeedback, ToutApp, and others.

We collect the email addresses of those who communicate with us via email, aggregate information on pages visitors access, and information volunteered by the visitor (such as survey information or form submissions) to improve the content of our web pages and the quality of our service. We may use contact information you provide on our website for marketing and sales purposes. We honor requests to opt out of marketing and sales communications; if you opt out, we will maintain your contact information in our "do not contact" list.

When you purchase or evaluate our products and services we may ask for information such as your name, company name, email address, billing address, and credit card information. We use information that you provide to deliver and bill for those products and services, identify and authenticate you, contact you, and other purposes like research for product improvement.

The information we collect is not shared with or sold to other organizations for commercial purposes, except to provide products or services you've requested, when we have your permission, or under the circumstances described in this policy.

## **Web Browser DNT Notice**

We only share your activity on our website with third parties according to the terms described above. Because the websites we operate do not collect or use the type of information that is generally subject to your browser's "Do Not Track" (DNT) privacy preference, our websites do not look for this signal from your browser. Your DNT settings, however, may affect the third-party services we use (listed above).

Your web browser's DNT setting does not affect data collection for the Services described in this policy, but the "Data Access, Correction, Deletion" section above describes how you may opt out of other data collection.

## **Our Policy Toward Children**

Our Services are not directed to persons under 13. If you become aware that your child has provided us with personal information without your consent, please contact us using the information below. We do not knowingly collect personal information from children under 13. If we become aware that a child under 13 has provided us with personal information, we take steps to remove such information using the opt-out process described above.

## **Changes and Contact Info**

From time to time, we need to make changes to our Privacy Policy to account for new features or for other reasons. When such changes occur, you are able to view the new document on our site. If you have concerns about our policy, let us know, and we'll try to respond promptly.

RetailNext  
Privacy Inquiries  
60 S. Market Street, Floor 10  
San Jose, CA 95113

privacy-inquiries@retailnext.net

## Prior Versions

Updated 1 June 2016 to explain our marketing program automation product, clarify which products are affected by the choice to opt out at <https://privacy.retailnext.net/>, and update Safe Harbor information based on the changes in that program. - [Link](#) - [PDF](#)

Updated 1 May 2015 to update Safe Harbor status for RetailNext, add a section header for opting out, and clarify that information you provide to us on our marketing website may be used for sales and marketing purposes. - [Link](#) - [PDF](#)

Updated 1 September 2014 to clarify that data retention policies apply to systems operated by RetailNext. Customers may retain data outside our systems according to their own policies. - [Link](#) - [PDF](#)

Updated 13 March 2014 to incorporate cloud service policies - [Link](#) - [PDF](#)

Previous version archived 12 March 2014 - [Link](#) - [PDF](#)

From Nearbuy Systems (prior to its acquisition by RetailNext):

Updated 1 July 2013 to update office address - [Link](#) - [PDF](#)

Updated 1 May 2013 - [Link](#) - [PDF](#)

Initial version effective 19 December 2012 - [Link](#) - [PDF](#)

The latest version is always at <http://retailnext.net/policies/privacy-policy/>, with a printable version [here](#).

You can also track and compare changes to our policies on GitHub at <https://github.com/retailnext/privacy-policy>.