AT&T Privacy Policy

EFFECTIVE DATE: JANUARY 1, 2023

Your information and your privacy are important — to you and to us. This policy explains how we use your information and how we keep it safe.

Importantly, it explains the choices you can make at any time about how your information is used.

When this Policy applies

This Privacy Policy ("Policy") covers the information generated when you use or subscribe to AT&T products, services, apps, websites or networks to which this Policy is linked. In the Policy, we call them "Products or Services" for short. They include voice, data, internet and other products, services and apps.

This Policy applies to you and anyone who uses our Products or Services under your account, except where we identify that separate AT&T privacy policies or terms and conditions apply. You are responsible for making sure all users under your account understand and agree to this Policy.

Here are special circumstances where this Policy may not apply, or may apply in addition to other policies:

- Some of our Products or Services – for example our FirstNet service – may be covered by their own privacy policies or additional privacy terms and conditions, while, U-verse TV is governed by the DIRECTV privacy policy.
- Some of our affiliates – such as DIRECTV and Cricket – have their own privacy policies that apply to data they collect from products, services and apps they provide. Any data collected subject to this Policy that is shared with those affiliates will still be treated consistent with this Policy.
- Some areas both inside and outside of the United States – for example California and the European Union – require us to adopt different policy terms and commitments in accordance with local laws.
- In certain cases, when you're using your AT&T Products or Services, other companies may be collecting information, so that your information may be covered by this Policy and other privacy policies at the same time. Here are some examples: if you purchase one of our Products or Services from a retailer; if you use our Services to connect to a social networking service or another company's Wi-Fi network; or if you provide your information to another company through a co-branded website, app or service controlled by the other company. In those cases, any information you provide to those companies may be subject to just their policy, or subject to both their policy and ours.
- If you are an AT&T business customer, we may have written Product or Service agreements that contain specific provisions about confidentiality, security or handling of information. When one of those agreements differs from or conflicts with this Policy, the terms of those agreements will apply instead.

The information we collect

We collect information about you and how you're using our Products or Services along with information about your devices and equipment. This may include performance information, along with web browsing, location and video viewing information.

Here are detailed examples of types of information we collect from our Products or Services:

- **Account Information** includes things like contact and billing information, service-related details and history and similar information, including Customer Proprietary Network Information. It also includes technical, equipment and usage information that relate to the services, products, websites and networks we provide you.

- **Web browsing and app information** includes things like the websites you visit or mobile apps you use. We use pixels, cookies, and similar technologies, and collect information on and off our network. We do not decrypt information you transmit using a secure website or app – including sensitive data like passwords or your banking information. We collect information including internet protocol and website address, and identifiers like advertising IDs and device IDs. This may also include information about the time you spend on websites or apps, the links or advertisements you see, the videos you watch online using our mobility and broadband services, search terms you enter, and items in your online shopping cart. We use this information together with data from testing and running our network.

- **Equipment Information** includes information that identifies or relates to equipment on our networks, such as type, identifier, status, settings, configuration, software or use.

- **Network performance and usage information** includes information about our networks, including your use of Products or Services or equipment on the networks, and how they are performing.

- **Location Information** includes your street address, your ZIP code and where your device is located. Location information is generated when the devices, Products or Services you use interact with cell towers, Wi-Fi routers, Bluetooth services, access points, other devices, beacons and/or with other technologies, including GPS satellites.

- **Biometric Information** such as unique biological pattern or characteristic or other unique physical or digital representation of biometric data, like a fingerprint, voiceprint, or scan of face geometry, that is used to identify a specific individual. To learn more, see AT&T's Biometric Information Privacy Notice.

How we collect your information

We collect your information in 3 ways:

- **You give it to us** when you make a purchase, set up an account or otherwise directly communicate with us.

- **We automatically get it** when you use, or your device uses, our Products or Services. For example, we use network tools to collect information like call and text records and the web browsing information we describe in this Policy.

- **We get it from outside sources** like credit reports, marketing mailing lists, and commercially available geographic and demographic information, along with other available information, such as public posts to social networking sites.

How we use your information

We use your information, together with the information from testing and running our network, to power our services and to improve your experiences. This information is used to provide, support, improve, protect, analyze and bill for our

products, service and network; to communicate with you about your service, products or apps; to better understand how you use our Products and Services; to market our services; to detect and avoid fraud; for advertising; and for research.

Here are examples of ways we use your information:

- Providing our Products and Services.
- Contacting you.
- Improving your experience and protecting the Products and Services we offer. This includes things like customer care, network security, verifying or authenticating your identity, detecting and preventing fraud, billing and collection, protecting your financial accounts, authorizing transactions and the development of future Products and Services.
- Helping us plan, deploy, improve, protect and defend our network infrastructure, protecting our property and legal rights, and for other lawful purposes.
- Understanding the Products, Services and offers that you, and other AT&T customers with whom you call and text and interact, might enjoy the most. We do not use the content of your texts, emails or calls for marketing or advertising.
- Helping us understand which Products, Services, and offers may interest you; creating engaging and customized experiences; and offering new or improved Products and Services to you. This is based on things like the information we've collected and our research, development and analysis.
- Designing and delivering advertising and marketing campaigns to you and others and measuring their effectiveness. You can manage your privacy choices, including opting in to the use of your web browsing and app information for advertising and marketing by participating in the Personalized Plus program.
- Delivering or customizing Products and the content you see, including advertisements, articles, videos, and marketing materials.
- Creating aggregate business and marketing insights, and helping companies develop aggregate insights (for instance, to market or improve Products and Services). We aggregate the data before we share it, which means that we group the information so that it does not identify you personally, and we require anyone who receives this data to agree they will only use it for aggregate insights, won't attempt to identify any person or device using this information, and will handle it in a secure manner, consistent with this Policy.
- For security purposes, including preventing and investigating illegal activities and violations of our Terms, Use Policies and other service conditions or restrictions.

How we share your information

- **We share it with your permission.**
- **We share it across AT&T companies.**
- **We share it with non-AT&T companies or entities as explained in this Policy**. For more details about how your information may be shared for advertising and marketing see Privacy Choices and Controls.

Sharing information across the AT&T affiliates

Like many large companies, AT&T is made up of many affiliates. Our Products and Services are developed, managed, marketed and sold by a variety of our affiliates. We share information that may identify you personally internally among our affiliates, such as DIRECTV and Cricket. For information collected under this Policy, we require the affiliate to use, share and protect the information consistent with this Policy including honoring your communications preferences for first-party marketing of their products and services, your advertising consents and your State Data Rights and Choices. We may also combine information that identifies you personally with data that comes from an app or affiliate that has a different privacy policy. When we do that, our Policy applies to the combined data set.

Sharing information with non-AT&T companies that provide services for us or for you

We share information that identifies you personally with vendors that perform services for us or that support Products or Services provided to you, including marketing or ad delivery services. We do not require consent for sharing with our vendors for these purposes. We do not allow those vendors to use your information for any purpose other than to perform those services, and we require them to protect the confidentiality and security of data they get from us in a way that's consistent with this Policy.

Sharing information with non-AT&T companies to enable Identity Verification

We may share information with non-AT&T companies for their purposes to provide you services such as verifying or authenticating your identity, detecting fraud, protecting your financial accounts, and authorizing transactions. We do not allow those non-AT&T companies to use it for any purpose other than to perform those services, and we require them to protect the confidentiality and security of data they get from us in a way that's consistent with this Policy. You are in control of this sharing. If you're an AT&T Prepaid customer, text "STOP" to 8010 to stop sharing with Identity Verification or "RESUME" to restart sharing at any time. Other customers can opt out of Identity Verification at att.com/PrivacyChoices.

Sharing information with other non-AT&T companies or entities

There are also times when we provide information that identifies you personally to other companies and entities, such as government agencies, credit bureaus and collection agencies, without your consent, but where authorized or required by law. Reasons to share include:

- Complying with court orders, subpoenas, lawful discovery requests and as otherwise authorized or required by law. Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits. You can find out more about this in our Transparency Report.
- Detecting and preventing fraud.
- Providing or obtaining payment for your service.
- Routing your calls or other communications.
- Ensuring network operations and security.
- Notifying, responding or providing information (including location) to a responsible governmental entity in emergency circumstances such as immediate danger of death or serious physical injury.
- Alerting the National Center for Missing and Exploited Children to information concerning child pornography of which we become aware through the provision of our services.

- Enforcing our legal rights, protecting our network and property or defending against legal claims.
- Complying with legal requirements to share the names, addresses and telephone numbers of non-mobile phone customers with phone directory publishers and directory assistance services. We honor your request for non-published or non-listed numbers.
- Providing name and number information for wireline and wireless CallerID and related services, like Call Trace. This means a person receiving a call can see the name and number of the caller.

Sharing Aggregate Metrics Reports with non-AT&T companies

Sometimes the services you enjoy from us directly involve other businesses. For example, we may collect information, including location and web browsing data, from visitors to places where we provide Wi-Fi services. In such cases, we aggregate the data before we use or share it with our business customers and service suppliers, which means that we group the information so that it does not identify you personally. We require that these metrics reports only be used for aggregate insights and that no one attempt to identify any person or device using this information. Consistent with this Policy, we also require that our metrics reports be handled in a secure manner and that the information included be used only for aggregate insights to enable the marketing or improvement of Products and Services.

Sharing Aggregate Insights

We may share insights with non-AT&T companies about AT&T's operations, network or services derived from aggregated customer data (data grouped so as not to identify you personally).

Sharing information for research

We may share information that doesn't identify you personally with other companies and entities for research. When we share this information, we require companies and entities to agree not to attempt or to allow others to use it to identify individuals. Our agreements will also prevent businesses from reusing or reselling the information, and require that they will handle it in a secure manner, consistent with this Policy.

Sharing information with AT&T affiliates and non-AT&T companies for advertising and marketing programs

We may share information with AT&T affiliates and with non-AT&T companies to deliver or assess effectiveness of advertising and marketing campaigns as described in Privacy Choices and Controls.

Sharing information to support location services

Location services rely on, use or incorporate the location of a device to provide or enhance the service. Location services may collect and use or share location information to power applications on your device (those that are pre-loaded or those that you chose to download), such as mapping and traffic apps, or other location services you subscribe to. AT&T will not share your location information for location services without your consent (to us or a company providing you service), except as required by law. If you purchase location services from another company, such as a medical alerting device company, the use or disclosure of location information is governed by the agreement between you and the service provider, including any applicable privacy policy of the service provider, and is not governed by this Policy. In other cases – for example parental controls services - the account holder for the location services, instead of a user, may initiate or subscribe to the location services and provide the required consent.

Your Privacy Choices and Controls

You can manage your privacy choices about how we contact you and how we use or share your information. You also have choices about how certain non-AT&T companies and advertisers use your information, including how we use and share your information for advertising and marketing.

Communication preferences

Sometimes we have offers or programs that may interest you. We'd like to be able to tell you about these. You can manage how we do it. You can opt-out of marketing and advertising programs, but we still may contact you with service and non-marketing messages.

- **Email:** You can opt-out of marketing emails by using att.com/marketing-unsubscribe.
- **Text messages:** Opt-out of our marketing text messages by replying "stop" to any message.
- **Consumer telemarketing:** Ask to be removed from our consumer telemarketing lists by contacting us at (800) 288.2020 (consumer) or (800) 321.2000 (business), or by sending an e-mail to privacypolicy@att.com and provide the phone number you wish to have removed. You also can ask the AT&T representative to remove you from our telemarketing lists when you receive a marketing or promotional call from us.
- **Business telemarketing:** Where required by local laws and/or regulations, we'll remove your business information from our telemarketing lists at your request.
- **National Do Not Call Registry:** The FTC maintains a National Do Not Call Registry at donotcall.gov, and some states in the United States may maintain their own Do Not Call Registry. Putting your number on these registries also may limit our telemarketing calls.
- **Automated messages:** In some cases, we will ask for your permission to send you automated calls or messages to your mobile phone. To opt-out of these calls or messages from us, go to manage your Automated Messages. As required or allowed by law, even if you opt-out, we may continue to contact you with automated calls or messages at the telephone number issued by us for certain important informational messages about your service. For example, we may need to let you know about a problem with your wireless service.
- **Postal mail:** You can review our Residential Do Not Mail Policy Statement and limit postal mail solicitations. You'll still receive billing statements, legal notices, product updates and other similar correspondence, and you may still receive some promotional mailings.
- **AT&T ActiveArmor:** You can also sign up for AT&T ActiveArmor to automatically block potential fraud calls, see warnings of suspected spam calls, add unwanted callers to your personal block list and help protect your phone from malware, viruses and system threats.

Choices about how we use and share your information for advertising and marketing

You have choices about how your information is used or shared in our programs that provide you with marketing and advertising tailored to your interests. As your provider of communications and internet services, our collection and use of information operates independently in many cases from the user controls and settings on your device, through your operating system, or on non-AT&T company websites or apps.

Online behavioral advertising: Online behavioral advertising is automated, customized advertising that you see when using online services, like ads in mobile apps or on websites. Those ads are served to you based on inferences about your interests. Those interests are determined from data collected about you, whether by AT&T or other parties.

- We work with ad companies that may serve ads across your use of online services. These companies may use cookies, mobile advertising identifiers, and other technologies to collect information about your use of our websites and other websites. This information may be used to, among other things, analyze and track online activities and deliver ads and content tailored to your interests as part of our advertising programs, such as our Personalized program.

- You can opt-out of online behavioral advertising from companies that participate in the Digital Advertising Alliance by going to their Consumer Choice Page or selecting this icon when you see it on an online ad.

- To limit collection of data on websites that may be used for advertising, you can manage cookies and other similar technologies on your computer. If you change computers, devices, web browsers or you delete cookies, you will need to opt-out again. Please note that our collection of web browsing information works independently of your web browser's privacy settings with respect to cookies and private browsing. In addition, we don't currently respond to Do Not Track, please go to All About Do Not Track for more information. You can manage AT&T's use of web browsing information at att.com/PrivacyChoices.

Personalized and Personalized Plus: Personalized and Personalized Plus both use information to deliver ads that we think you might be interested in on websites, apps and other properties, sites or services.

- **Personalized:** This program gives you the benefit of offers and ads that are relevant to your interests. To determine your possible interests, we use and share with advertising partners data about your use of our Products and Services. We also use data we get from our advertising partners, and demographic data like ZIP code and age range. You won't see more ads – just customized ads. The Personalized program does not use your precise location, web browsing data collected as an internet service provider, information about your medical conditions, financial account information, or Customer Proprietary Network Information. It also does not access or use the contents of your texts, emails or calls. The Personalized program may place you into general categories of interest, such as "soccer fan." When you participate in this program, we will also:

  - Use automated decision-making, such as artificial intelligence, for things like marketing and advertising.

  - Use some types of Sensitive Personal Information, like your ethnic or racial origin, for things like marketing and advertising, except as noted above. But for customers in Colorado, Connecticut, and Virginia, we will only do so if you are also participating in Personalized Plus.

You will be included in the Personalized program unless you opt out. You may opt-out by going to att.com/PrivacyChoices.

- **Personalized Plus:** With your consent, you may participate in Personalized Plus, which gives you the benefit of offers and ads that are relevant to your interests. To determine your possible interests, we use and share with advertising partners data about your use of our Products and Services – such as web browsing and apps. We also use data we get from our advertising partners, and demographic data like ZIP code and age range. In addition, by using information from testing and running our network, we may infer websites visited or videos viewed over a secure connection for advertising and marketing purposes. You won't see more ads – just customized ads. You may opt in to this program by going to att.com/PrivacyChoices.

  - Personalized Plus also uses your precise location and Customer Proprietary Network Information for more customization. It does not access or use the contents of your texts, emails or calls.

- If you live in Colorado, Connecticut or Virginia, by participating in Personalized Plus, you agree to let us collect, use, store and share some types of Sensitive Personal Information, like your race or ethnic origin. If you live in other states, we collect, use, store and share this data by default to serve you custom ads; you can manage your preferences by opting out of the Personalized Program at att.com/PrivacyChoices.

- All customers participating in the Personalized Plus are automatically opted in to the Personalized program. You can make changes at any time by going to att.com/PrivacyChoices.

Other Choices

- **Customer Proprietary Network Information (CPNI):** You can learn more about CPNI and your choices about our use of that information for marketing purposes here.

  - If you don't want us to use your CPNI internally for things like offers, here is what you can do:

    - Login to att.com/PrivacyChoices.

    - Opt-out at att.com/cpni/optout.

    - Call us at (800) 315.8303, any time of day, and follow the prompts.

    - Chat with a service representative at (800) 288.2020 (consumer) or (800) 321.2000 (business).

- Identity Verification: We may share information with non-AT&T companies such as your bank to help protect your accounts from fraud, verify your identity and make sure you authorize certain transactions. We do not allow those non-AT&T companies to use your information for any other purpose than those services. You are enrolled by default, but you can stop at any time. Text "STOP" to 8010 to turn off Identity Verification or "RESUME" to restart. Or manage your choices at att.com/PrivacyChoices.

Security

We work hard to safeguard your data using a range of technological and organizational security controls.

We maintain and protect the security of computer storage and network equipment, and we use security procedures that require employees to authenticate themselves to access sensitive data. We also limit access to personal information only to those with jobs requiring such access. We require callers and online users to authenticate themselves before providing account information.

No security measures are perfect, however. We can't guarantee that your information will never be disclosed in a manner inconsistent with this Policy. If a breach were to occur, we will notify you as required by applicable law.

Data storage, transfer, retention and accuracy

We take steps to ensure that data is processed according to this Policy and to the requirements of applicable law of your country and of the additional countries where the data is subsequently processed.

Data we collect may be processed and stored in the United States or in other countries where we or our affiliates or service providers process data.

When we transfer personal data from the European Economic Area to other countries, we use a variety of legal mechanisms to help ensure all applicable laws, rights and regulations continue to protect your data.

We keep your information as long as we need it for business, tax or legal purposes. We set our retention periods based on things like the type of personal information collected, how long the personal information is needed to operate the business or provide our Products and Services and whether the business is subject to contractual or legal obligations – such as ongoing litigation, mandatory data retention laws or government orders to preserve data relevant to an investigation. After that, we destroy it by making it unreadable or indecipherable.

Need to update your information? We're happy to help you review and correct the information we have on your account and billing records. For more information, please see the Contact Us section of this Policy.

Other privacy information

Changes in ownership or to the Policy

Information about our customers and users, including information that identifies you personally, may be shared and transferred as part of any merger, acquisition, sale of company assets or transition of service to another provider. This also applies in the unlikely event of an insolvency, bankruptcy or receivership.

We may update this Policy as necessary to reflect changes we make and to satisfy legal requirements. We'll post a prominent notice of material changes on our websites. We'll give you reasonable notice before any material changes take effect.

Information specific to Business Customers

AT&T will not use our Business Customers' User information for any marketing or advertising purposes other than to market enterprise Products and Services including apps, services, and supporting devices. However, we may use your Business Customer relationship (but not any other information about you or your Business Customer services) to qualify you for certain offers on AT&T's consumer Products and Services. Keep in mind that AT&T sells a variety of Products and Services to small and large business customers alike. Should a customer be unsure of their account status, they can call the toll free number on their bill to verify if the Product they purchase is billed as a business or consumer Service.

Information specific to children

We don't knowingly collect personal information from anyone under the age of 13 without parental notice and, where appropriate, parental consent. Unless we have parental consent, we will not contact a child under the age of 13 for marketing purposes. We and our advertising partners may collect, use or share information about customers who log onto our websites and/or email accounts as described in the Information we collect, how we collect your information, how we use your information and how we share your information sections of this Policy. You can manage your account, including information about subaccount holders by logging on to manage your account.

Information collected from devices or services purchased by adult subscribers that are used by children without our knowledge will be treated as the adult's information under this Policy.

We have developed safety and control tools, expert resources and tips designed to help you manage technology choices and address online safety concerns. Please go to AT&T Screen Ready for more information.

Information for our California customers

Website data collection:

We don't knowingly allow other parties to collect personally identifiable information about your online activities over time and across non-AT&T company websites for their own use when you use our websites and services, unless we have your consent.

Do Not Track notice:

We don't currently respond to Do Not Track. Please go to All About Do Not Track for more information. However, we recognize and honor the opt out preference signal associated with a Global Privacy Control.

California customers have the right, in certain circumstances, to request information about whether a business has disclosed Personal Information to any third parties for their direct marketing purposes. You have the right to opt out of our disclosing your information to third parties for their marketing purposes. To find out more, go to att.com/PrivacyChoices.

State Privacy Rights and Choices

Certain states provide you rights regarding your Personal Information. Personal Information and rights in these states and jurisdictions, are explained in the following section. To underscore our commitment to our privacy principles and to provide a consistent experience, we also offer these as choices to consumers in places where they are not required:

Personal Information ("Personal Information") means information that identifies, relates to, describes, is reasonably capable of being associated with, is linked to or could be reasonably linked to, either directly or indirectly, an identified or identifiable individual or household.

The Personal Information We Collect and Purpose for Collection

Categories	Examples	Collected or created	Source	Purpose of collection and use
Identifiers	Name, postal address, email address, account name, Social Security number, driver's license number, passport number, taxpayer identification number, IP address, device IDs	• Collected	• Consumers give it to us • We automatically get it • We get it from outside sources	• Offer, market, advertise or provide Products and Services • Provide to or receive information from credit reporting agencies • Enable billing and payment processing • Prevent fraud • Enable cross-context behavioral or targeted advertising • Conduct research

Characteristics of protected classification under state or federal law	Age, age range, date of birth, gender, preferred language, marital status	• Collected	• Consumers give it to us • We get it from outside sources	• Offer, market, advertise or provide Products and Services • Receive information from credit reporting agencies • Prevent fraud • Enable cross-context behavioral or targeted advertising • Conduct marketing research and analytics
Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies	• Collected and created	• We automatically get it • We get it from outside sources	• Offer, market, advertise or provide Products and Services • Provide information to or receive information from credit reporting agencies • Enable billing and payment processing • Prevent fraud • Enable cross-context behavioral or targeted advertising • Conduct research
Geolocation data	Street address, ZIP code and device location	• Collected	• Consumers give it to us • We automatically get it	• Offer, market, advertise or provide Products and Services • Prevent fraud • Receive information from credit reporting agency • Enable cross-context behavioral or targeted advertising • Conduct research • Perform analytics

Internet or other electronic network activity information	Browsing history, search history and information regarding an individual's interaction with an internet website, application, or advertisement	• Collected and created	• We automatically get it	• Offer, market, advertise or provide Products and Services • Prevent fraud • Enable cross-context behavioral or targeted advertising • Conduct research
Inferences or audience segmentation	Individual profiles, preferences, characteristics, behaviors	• Collected and created	• Consumers give it to us • We automatically get it • We get it from outside sources	• Offer, market, advertise or provide Products and Services • Enable billing and payment processing • Prevent fraud/authenticate identity • Enable cross-context behavioral or targeted advertising • Conduct research
Audio, electronic, visual or similar information	Video surveillance, audio recordings, photographs, signatures associated with an account	• Collected	• We automatically get it • Consumers give it to us	• Provide security services • Prevent fraud/authenticate identity • Enable billing and payment processing • Enable quality control of providing Products and Services • Conduct research
Biometric information	Fingerprint, voiceprint, or scan of face geometry, that is used to identify a specific individual	• Collected and created	• Consumers give it to us	• Prevent fraud and provide identity verification
Education information	Degree(s), actual or inferred level of education	• Collected	• Consumers give it to us • We get it from outside sources	• Offer, market, advertise or provide Products and Services • Enable cross-context behavioral or targeted advertising • Research

Professional or employment-related information	Current or past employment history, licenses and professional membership	• Collected	• Consumers give it to us • We get it from outside sources	• Offer market, advertise or provide Products and Services • Enable cross-context behavioral or targeted advertising • Research

Information We Shared About Consumers

Here is information about the Personal Information we have collected over the past year and the purpose for which we shared or sold it. Note, some states define "sale" very broadly and include the sharing of Personal Information for anything of value. According to this broad definition, in the year before the date this policy was updated, we have sold or shared the following categories of Personal Information about at least some consumers:

Categories	Collected or created	Categories of companies we've shared with	Purpose for sharing	Purpose for selling
Identifiers	Collected	• Product and services delivery companies • Marketing services companies • Cloud storage companies • Credit reporting agencies • Billing, payment processing and collection companies • Fraud prevention and authentication/identity verification entities • Analytics companies • Affiliates • Research entities	• Product and services delivery • Marketing and advertising services • Data storage • Analytics and measurement • Fraud prevention/ identity verification • Billing, collections and payment processing • Cross-context behavioral or targeted advertising • Credit scoring and reporting • Research	• Marketing and advertising

Characteristics of protected classification under state or federal law	Collected	• Cloud storage companies • Credit reporting agencies • Fraud prevention and authentication/identity verification entities • Analytics companies • Research entities	• Data storage • Credit scoring and reporting • Fraud prevention/ identity verification • Analytics and measurement • Research	• Not sold
Commercial information	Collected	• Product and services delivery companies • Marketing services companies • Cloud storage companies • Credit reporting agencies • Billing and payment processing companies • Fraud prevention and authentication/identity verification entities • Analytics companies • Affiliates • Research entities	• Product and services delivery • Marketing and advertising • Data storage • Analytics and measurement • Fraud prevention/ identity verification • Cross-context behavioral or targeted advertising • Billing, collections and payment processing • Research	• Marketing and advertising
Internet or other electronic network activity information	Collected	• Marketing services companies • Analytics companies • Cloud storage companies • Research entities	• Marketing and advertising • Analytics and measurement • Cross-context behavioral or targeted advertising • Data Storage • Research	• Not sold

Geolocation data	Collected	• Product and services delivery companies • Marketing services companies • Cloud storage companies • Billing and payment processing companies • Fraud prevention and authentication/identity verification entities • Analytics companies • Affiliates • Credit reporting agencies • Research entities	• Product and services delivery • Marketing and advertising • Data storage • Billing, collections and payment • Fraud prevention/ identity verification • Analytics and measurement • Research	• Marketing and advertising (does not include Precise Geolocation)
Inferences or audience segmentation	Collected and created	• Marketing services companies • Cloud storage companies • Analytics companies • Research entities	• Marketing and advertising • Data storage • Analytics and measurement • Research	• Not sold
Audio, electronic, visual or similar information	Collected	• Cloud storage companies • Fraud prevention/security companies • Research entities	• Data storage • Fraud prevention/security • Research	• Not sold
Biometric information	Collected	• Fraud prevention and authentication/identity verification entities	• Fraud prevention/identity verification	• Not sold

Education information	Collected	• Research entities	• Research	• Not sold
Professional or employment-related information	Collected	• Credit reporting agencies • Fraud prevention and authentication/identity verification entities • Research entities	• Fraud prevention/ identity verification • Credit scoring and reporting • Research	• Not sold

The Sensitive Personal Information We've Collected and the Purpose of its Collection, Sharing and Sale

Here is information about the Sensitive Personal Information, as defined under California law, that we have collected about consumers over the past year. We list the purpose for which we collected it, the types of companies we've shared it with and why. AT&T has not sold Sensitive Personal Information.

Categories	Purpose for collection	Categories of companies we've shared with	Purpose for sharing (making available constitutes a share)
Gov't IDs: Social Security, driver's license, state Identification card, or passport number	Provide information to or receive information from credit reporting agencies Prevent fraud/ authenticate identity	• Cloud storage companies. • Credit reporting agencies • Fraud prevention and authentication/identity verification entities	• Report to or receive information from credit reporting agencies • Prevent fraud /provide identity verification
Financial accounts & credentials: account log-In, financial account, debit .card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account	• Enable billing and payment processing	• Not Shared	• Not Shared

Precise geolocation	• Offer or provide Products and Services • Prevent fraud • Enable location and emergency services • Conduct research	• Product and services delivery companies • Cloud storage companies • Fraud prevention and authentication/identity verification entities • Research entities (Provided in aggregate)	• Offer, market, advertise or provide Products and Services • Provide location services • Prevent fraud • Research
Demographic, religious or occupational information: racial or ethnic origin, religious or philosophical beliefs, or union membership	• Offer or provide Products and Services • Conduct research and development • Prepare aggregate insights	• Marketing services companies • Analytics companies • Research entities	• Offer, market, advertise or provide Products and Services • Enable cross-context behavioral or targeted advertising • Research
Content of communications: The contents of an individual's Plain SMS text messages up to 48 hours and spam texts [Learn More], unless AT&T is the intended recipient of the communication	• Network Operations	• Not Shared	• Not Shared
Biometric information: the processing of biometric Information for the purpose of uniquely identifying an individual	• Prevent Fraud	• Fraud prevention and authentication/identity verification entities	• Prevent fraud/ provide identity verification

You can tell us not to sell or share your Personal Information. Additionally, you can tell us to limit the use of your Sensitive Personal Information. You may make such requests by:

- Visiting www.att.com/PrivacyChoices and opting out of the sharing and selling of your personal information and opting out of the Personalized program to limit the use of your Sensitive Personal Information; or
- Visiting our Choices and Controls page and selecting the Do Not Sell or Share or the Control Sensitive Personal Info Request; or
- Contacting us at 866-385-3193.

Providing Personal Information to service providers or contractors does not constitute a sale or sharing of Personal Information. You may use an authorized agent to make your request and we will confirm whether or not your request has been processed and why.

Once we receive and verify your request, we will not sell or share your Personal Information and will limit the use of your Sensitive Personal Information unless you later allow us to do so. We may ask for your permission to resume sale of your Personal Information at a later date, but we will wait at least 12 months before doing so.

Consumers Under 16 Years Old

We do not have actual knowledge that we sell Personal Information of consumers under 16 years of age. If we collect Personal Information that we know is from a child under 16 years old, we will not sell that information unless we receive affirmative permission to do so. If a child is between 13 and 16 years of age, the child may provide that permission.

Your Right To Request Disclosure Of Information We Collect And Share About You

We are committed to ensuring that you know what information we collect. You can ask us for the following information:

- The categories and specific pieces of your Personal Information we've collected.
- The categories of sources from which your Personal Information was collected.
- The purposes for collecting or selling your Personal Information.
- The categories of non-AT&T companies with whom we shared your Personal Information.

We are also committed to ensuring that you know what information we share about you. You can submit a request to us for the following additional information:

- The categories of Personal Information we've sold about you, the categories of non-AT&T companies to whom we've sold that Personal Information, and the category or categories of Personal Information sold to each non-AT&T company.

The categories of Personal Information that we've shared with service providers that provide services for us, like processing your bill; the categories of service providers to whom we've disclosed that Personal Information; and the category or categories of Personal Information disclosed to each service provider.

To exercise your right to request the Personal Information that we collect or share, either visit our Choices and Controls page or contact us at 866-385-3193. These requests are generally free and are provided in a format that is portable in a readily usable format.

Your Right to Request Correction of Inaccurate Personal Information

You may request that we correct inaccurate Personal Information we have about you. When you request that we correct inaccurate information, we will ask you to provide documentation supporting the accuracy of the Personal Information that is the subject of your request, and in doing so we will evaluate the totality of the data relating to the contested Personal Information. We may deny your request if we determine that the contested Personal Information is more likely than not accurate based on the data provided. Whether or not we are able to honor your correction request, we will notify you that your request was processed or denied and why. To exercise this right or choice, either visit our Choices and Controls page or contact us at 866-385-3193.

Your Right To Request The Deletion Of Personal Information

Upon your request, we will delete the Personal Information we have collected about you, except for situations when that information is necessary for us to: provide you with a good or service that you requested; perform a contract we entered into with you; maintain the functionality or security of our systems; comply with or exercise rights provided by the law; or use the information internally in ways that are compatible with the context in which you provided the information to us, or that are reasonably aligned with your expectations based on your relationship with us.

To exercise your right to request the deletion of your Personal Information, either visit our Choices and Controls page or contact us at 866-385-3193. Requests for deletion of your Personal Information are generally free.

Your Right To Appeal

You can ask us to reconsider on the outcome of a request you've submitted regarding your rights to access, correction, deletion and portability of your Personal Information and/or the right to know whether your personal data is being sold or shared. Upon receipt of your appeal, we'll research your request and provide you an explanation of our review in writing.

Verification of Identity — Access, Deletion or Correction Requests

Password Protected Account. If you maintain a password-protected account with us, in most cases you may submit an access, deletion or correction request by authenticating yourself with a password like you would when you access your account (see exceptions below in the following paragraph). You'll have to authenticate yourself again to access your data or submit your deletion request.

Former Accountholders, Non-Accountholders (without a Password Protected Account) – and also FirstNet, Prepaid and .net accounts. If you do not have a password protected account – or have a FirstNet, prepaid or .net account – we will ask to verify your identity using our mobile verification process. This process may involve a one-time pin or the capture of an image of your identity document, such as your driver's license, and compares it to a self-photo you submit. We will only use this information to verify your identity. We will delete it after the time expires allowed by applicable state laws to process and respond to your request.

If we cannot verify your identity, we will notify you that we will not be able to respond to your request.

Authorized Agents

You may designate an authorized agent to submit requests on your behalf. Your agent will need a valid power of attorney or written permission signed by you. If the agent relies on written permission, we'll need to verify the agent's identity. We may also contact you directly to confirm the permission. Your authorized agent can submit your requests by calling us at 866-385-3193.

We Don't Mind If You Exercise Your State Data Rights

We are committed to providing you with control over your Personal Information. If you exercise any of these rights explained in this Privacy Policy, we will not disadvantage you. You will not be denied or charged different prices or rates for goods or services or provided a different level or quality of goods or services.

Questions

Any consumer who wishes to request further information about our compliance with these requirements, or who has questions or concerns about our privacy practices and policies, can email us at privacypolicy@att.com, or write to us at

AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 2100, Dallas, TX 75202.

Data Retention

AT&T decides how long to retain your Personal Information consistent with these criteria:

- The type of personal information collected;
- How long the personal information is needed to operate the business or provide our Products and Services; and
- Whether the business is subject to contractual or legal obligations – such as ongoing litigation, mandatory data retention laws or government orders to preserve data relevant to an investigation.

View California Metrics For The Prior Calendar Year

You may review information about the company's California data requests for the prior calendar year by visiting the California metrics page.

Customer Proprietary Network Information (CPNI)

CPNI is information about your telecommunications services from us, like the plan you subscribe to and details about who you've called. But your telephone number, name and address are not CPNI.

We use your CPNI internally. For example, we may share CPNI with AT&T affiliates and our agents to offer new services or promotions. We use your CPNI to create aggregate data or information that does not personally identify you.

We do not share CPNI with anyone outside of the AT&T affiliates or our authorized agents or vendors without your consent, with the following authorized exceptions: Court orders; as authorized by law; fraud detection; to provide your service and route your calls; for network operations and security; aggregate information and information that doesn't identify you personally.

It is your right and our duty under federal law to protect the confidentiality of your CPNI.

If you don't want us to use your CPNI internally for things like offers, here is what you can do:

- Login to att.com/PrivacyChoices.
- Opt-out at att.com/cpni/optout.
- Call us at (800) 315.8303, any time of day, and follow the prompts.
- Chat with a service representative at (800) 288.2020 (consumer) or (800) 321.2000 (business).

If you choose to restrict our use of your CPNI, it won't affect your ability to use any of your services. You can change your mind at any time about letting us use or not use your CPNI. If you restrict your CPNI use, you may still get marketing from us about products and services similar to those you purchase from us.

How to contact us about this Policy

Contact us at either of these addresses for any questions about this Policy.

- E-mail us at privacypolicy@att.com.

- Write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 2100, Dallas, TX 75202.

For questions not related to privacy click on the "Contact Us" link at the bottom of any att.com page. You also can access your online account from the upper right hand corner of our home page at att.com for additional service options.

If you are not satisfied with our resolution of any dispute, including with respect to privacy or data-use concerns, please review a description of our dispute resolution procedures at https://www.att.com/help/notice-of-dispute/.

You also have the option of filing a complaint with the FTC Bureau of Consumer Protection, using an online form, or by calling toll-free 877.FTC.HELP ((877) 382.4357; TTY: (866) 653.4261). Other rights and remedies also may be available to you under federal or other applicable laws.

Customer service contact numbers can be found at att.com.

Affiliates

Below is a list of some of the affiliates publicly recognized to be part of the AT&T family of companies that have access to information collected from users and subscribers to products, services, apps, websites, or networks provided by AT&T Communications, as set forth in the AT&T Privacy Policy. This list is not exhaustive and may be subject to change.

Publicly Recognized, Non-AT&T branded affiliates of AT&T including but not limited to the following:

- DIRECTV, LLC and its affiliates,
- Non-AT&T branded affiliates of AT&T Communications, which include, but are not limited to: Cricket entities, Wayport LLC, NavLink Inc., etc.

AT&T Communications Companies (domestic and international), which include but are not limited to the following:

- AT&T Mobility companies and all affiliates,
- AT&T landline and broadband companies (e.g. AT&T California, AT&T Wisconsin, etc.) and other similar AT&T communication companies (e.g. AT&T Long Distance, AT&T Messaging, LLC)

Affiliates of AT&T Latin America:

- AT&T Comunicaciones Digitales, S. de R.L. de C.V., AT&T Comercialización Móvil, S. de R. L. de C.V.

Biometric Information Privacy Notice

In addition to the information provided in the AT&T Privacy Policy, we want to help you better understand how AT&T treats Biometric Information.

Biometric information is a unique biological pattern or characteristic or other unique physical or digital representation of biometric data, like a fingerprint, voiceprint, or scan of face geometry, that is used to identify a specific individual. We may use Biometric Information for purposes that include verifying or authenticating your identity, detecting and preventing fraud and safety or other security purposes.

AT&T will only retain Biometric Information until the initial purpose for collecting it has been satisfied or within three

years of the individual's last interaction with AT&T, whichever occurs first, unless legally required to keep it for a different period.

If you have a question about how this notice applies, contact privacypolicy@att.com.