DTC WIFI+ MOBILE APPLICATION PRIVACY POLICY

What is covered by this Privacy Policy

DTC WiFi+ is an application developed by Calix, Inc. for use by subscribers of broadband service providers (BSPs) who purchase cloud and software services from Calix, Inc. Calix, Inc. is a processor of (or service provider for) its BSP's subscriber personal information under applicable privacy and data protection laws. Your BSP provider is the controller of (or business for) its subscriber personal information. In other words, your BSP determines how and why your information is processed. As such, subscribers should refer to their BSP's privacy notice for details on how the BSP processes subscriber personal information.

Privacy Policy applies for any use of the App

This Privacy Policy applies to the App described in the WiFi+ Mobile Application End User License Agreement (the "**Agreement**"). Please read your BSP's privacy notice and this Privacy Policy carefully to understand how information collected by the App will be treated. If you do not agree with your BSP's privacy notice and this Privacy Policy, you should not install, use, or access the App.

How Calix Collects Your Information

On behalf of your BSP, Calix collects and processes information provided directly by you when you install the App and register for an account to use the App. Specifically, this information includes:

- Your name, email address, password/pin, preferred language, and your account number with your BSP;
- Information about the equipment deployed at your premises that you choose to connect to the App such as the MAC address, serial number or other unique identifier for your router;
- Data insights Calix attains based on correlation and analytics of your information collected in providing the App, and user-associated analytics to improve the quality of the app experience.

Categories of Data

Below is a summary of the categories of personal information that we have collected in the course of providing our Services in the last 12 months.

Category	Examples	Collected	Business Purpose
A. Identifier	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes	Provide BSP services
B. Personal Information categories listed in the California Records statue	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license, or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	Yes	Provide BSP services
C. Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	No	Not collected
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	No	Not collected
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No	Not collected

F. Internet or similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	Yes	Product Improvement
G. Geolocation data	Physical location or movements	Yes	Federal funding reporting
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	No	Not collected
I. Professional or employment-related information	Current or past job history or performance evaluations.	No	Not collected
J. Non-public education information	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary codes.	No	Not collected
K. Inferences drawn from other personal information	Profile a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	No	Not Collected
A. Government identifiers	Social security, driver's license, state identification card, or passport number.	No	Not collected
B. Complete account access credentials	Usernames, account numbers, or card numbers combined with required access/security code or password.	Yes	Provide BSP services
C. Precise geolocation	Your geolocation is within a radius of 1,850 feet.	Yes	Federal funding reporting
D. Racial or ethnic origin	Information regarding your race or ethnicity.	No	Not collected

E. Religious or philosophical beliefs	Information regarding your religious or philosophical beliefs or practices.	No	Not collected
F. Union membership	Whether or not you are a union membership.	No	Not collected
G. Genetic data	Data pertaining to your DNA or genes.	No	Not collected
H. Mail, email, or text message contents not directed to us	Contents of any message that is not sent to Calix.	No	Not collected
I. Unique identifying biometric information	Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	No	Not collected
J. Health, sex, life, or sexual orientation information	Information pertaining to your health, fitness, sexual orientation or identity or expression	No	Not collected

How Calix Uses the Information

On behalf of your BSP, Calix uses the information collected as described in this Privacy Policy, to:

- Provide you with the App and the Services/notifications provided through the App as described in the Agreement;
- Implement, improve and/or enhance the App or to provide App features, including to make future releases available to you;
- Carry out Calix's obligations as described or authorized in the Agreement, your BSP's privacy notice, and this Privacy Policy;
- Enforce Calix's rights arising from the Agreement between you and Calix; and
- Fulfill any other purpose authorized by you and reasonably required for the App.

Your BSP may also use the information collected as described in this Privacy Policy, to inform you about goods and services that may be of interest to you.

Promotional Tiles

The App may display promotional tiles within the user interface. These tiles may include content such as product offers, service recommendations, or application updates from the BSP or other providers authorized by the BSP. These tiles are not personalized, are not based on your personal information or application activity and are all the same for all users. No user data is collected or used to target or optimize these promotions. If the BSP ever decides to personalize promotional content in the future, the applicable privacy policies will be updated, and the BSP will seek your consent where required.

You may opt-out of receiving promotional tiles by updating your preferences in the App settings.

Disclosure of Information

Calix does not sell or otherwise distribute or disclose your information to third parties other than as described or authorized in the Agreement, including this Privacy Policy.

Calix discloses the information to its subsidiaries, affiliates and certain third-party vendors and contractors that provide development, integration, web hosting and consulting services to Calix to provide you with the App, to maintain, support, develop, improve and/or enhance the App and to fulfill Calix obligations associated with the App.

Your BSP or Calix may be required to disclose information under certain circumstances:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request;
- To enforce Calix's rights arising from the Agreement entered into between you and Calix;
- If either the BSP or Calix believes disclosure is necessary or appropriate to protect their rights, property, or the safety of their customers or other third parties; or
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Calix's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which your information and/or your subscriber information held by the BSP or Calix are among the assets transferred.

Children Under the Age of 16

The App is not intended for children under 16 years of age, and on behalf of its BSPs, Calix does

not knowingly collect personal data of children under 16, without parental consent. If Calix learns that personal data from a child under 16 has been obtained or received without verification of parental consent, Calix will delete that information. If you believe Calix might have any information from or about a child under 16, please notify Calix by completing a Request Formopens in a new tab (clicking the link will take you to TrustArc, whom Calix has engaged to assist with personal information requests).

Data Security

All information you provide to us is stored on our secure servers behind firewalls. Calix utilizes mechanisms such as intrusion detection systems, intrusion prevention systems, firewalls and encryption to secure information from accidental loss and from unauthorized access, use, alteration, and disclosure.

Calix deploys Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to alert and proactively contain potential threats. Enhanced security visibility and coverage is enabled through added layers of firewall and IDS beyond the network perimeter.

Management connections to servers are always authenticated and encrypted via Secure Shell (SSH) when administration access is required for troubleshooting, patch management, and upgrades.

Calix runs automated vulnerability scanning on all perimeter systems to identify potential security risks. Scanning applications are regularly updated to remain current and up to date on important security vulnerabilities. Patches are applied to all relevant systems unless a compensating control is implemented.

Calix uses a variety of industry-standard security technologies and best practices to help protect information from unauthorized access, use, or disclosure. All data stored on the Calix systems is encrypted following industry standards using the strongest keys and ciphers. All communications with the App are protected with industry standard security protocols.

You control access to your account. You must keep your login credentials and passwords secure and protected and maintained as confidential. Calix is not responsible for any circumvention of any privacy settings or security measures provided.

Your Choices About Our Collection, Use, and Disclosure of Information

Depending on your jurisdiction and the type of data collected, you may have the following rights with respect to your personal information depending on the applicable state consumer privacy laws.

a. Notice.
b. Access.

c. Correction.
d. Deletion.
e. Opt-out of sale or sharing of personal information.
f. Limit use of sensitive personal information.
g. Portability.
h. Opt-out of automated decision-making and profiling.
i. Appeal.
j. Non-discrimination.

To access, review or correct any information, please contact the BSP or you can exercise your rights by clicking the Request Form link in the "Contacting Us" section below.

Other California Privacy Rights

The State of California also grants California residents privacy rights unrelated to the California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act ("CPRA"). Those rights include the California "Shine the Light Law" (Civil Code Section § 1798.83), which permits California residents to request certain information regarding our disclosures of personal information to third parties for their direct marketing purposes. Calix does not disclose personal information to third parties for their direct marketing purposes.

Changes to this Privacy Policy

The date the Privacy Policy was last revised is identified at the end of this Privacy Policy. You are responsible for periodically visiting this Privacy Policy to check for any changes.

Contact Information

For questions about your service, please contact your BSP directly. To ask questions or comment about this Privacy Policy and Calix's privacy practices for the Cloud Services provided to your BSP, contact your BSP or complete this Request Form (clicking the link will take you to TrustArc, whom Calix has engaged to assist with personal information requests).