Privacy Charter

Prepared by Tutela Technologies Ltd.

Hunter Macdonald, CEO
Devan McCannel, Mobile Partnerships Manager, and
Anthony Kroeker, VP Engineering Systems & Data Protection Officer

Tutela’s privacy controls and practices have been reviewed, on the basis of a Privacy Assessment, by PricewaterhouseCoopers

Last updated: January 2, 2019
Tutela Privacy Charter

As a company whose livelihood depends on data and its proper treatment, Tutela takes data privacy and security very seriously. As such we have taken steps to go well beyond basic privacy and data protection requirements.

Tutela collects many statistics and measurements, but we do not collect any personal information that is directly attributable to individuals. Our products and services do not require user identification. We take both commercial and technical steps to ensure that our datasets are not used by Tutela, our partners, or our customers, to identify individuals.

Why we collect data.

Tutela is a world leader in improving wireless networks based on users’ perspective of performance. We collect data so that we can help wireless service providers and other third parties better analyze and communicate consumer mobile trends, understand the drivers of subscriber churn and acquisition, design effective marketing campaigns, and improve your wireless networks.

We typically use data to identify areas where there are poor WiFi or cellular signals so that wireless carriers can fix their network issues and improve performance for their subscribers.

How we collect data.

Collecting data from millions of devices is a significant challenge. Our research showed that users did not want to install more applications on their devices to collect data, but were happy to provide pseudo-anonymous data if it helped to reduce advertisements, improve mobile signals, and if it did not affect their experience or device performance.

Our software runs in the background of popular mobile apps and games to collect data. This helps us to collect as much useful data as possible, without requiring the user to download another application. In many cases, this also means that the mobile apps can display fewer advertisements to users because we pay the mobile application to partner with us.

All of our mobile application and games partners are required to provide disclosures and permission requests to their users to enable pseudo-anonymous data collection, and abide by all relevant global privacy legislation and app store guidelines. Tutela regularly audits our partners to ensure compliance.
What data we collect.

All information we collect is kept pseudo-anonymous or anonymous at all times – meaning that separate data sets, not held or processed by Tutela, are required to identify individuals. Tutela ensures that this attribution is both difficult and strictly prohibited through licensing provisions.

Tutela’s application partners configure the Tutela data collection library based on their data collection user permissions, user disclosures, and data policy. The information actually collected by Tutela may differ on a case-by-case basis based on this partner configuration.

This information includes:

<table>
<thead>
<tr>
<th>Category</th>
<th>Typical Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device &amp; Environment Characteristics</strong></td>
<td>Wireless device details are required to identify if specific network issues are limited to a device type or indoor/outdoor environments.</td>
</tr>
<tr>
<td>Examples: Device Make, Model, OS Version, Screen Resolution, Lux</td>
<td></td>
</tr>
<tr>
<td><strong>Geolocation</strong></td>
<td>Required to aggregate and plot network performance on a map to convey network coverage.</td>
</tr>
<tr>
<td>Typically expressed as latitude-longitude coordinates</td>
<td></td>
</tr>
<tr>
<td><strong>Connection Details</strong></td>
<td>Used to separate data and results by operator and compare their performance, and congestion, to help with competitive analysis.</td>
</tr>
<tr>
<td>E.g. Service Provider Name, Cell Tower Name, Roaming Details, MB Used</td>
<td></td>
</tr>
<tr>
<td><strong>Connection Quality</strong></td>
<td>Used to evaluate the performance of wireless networks.</td>
</tr>
<tr>
<td>E.g. Download Speed, Network Latency, Signal Strength</td>
<td></td>
</tr>
<tr>
<td><strong>Video and media service performance</strong></td>
<td>Used to evaluate wireless networks, and common services such as video. Test videos are downloaded in the background. Videos selected by consumers for viewing are not monitored or tested for performance.</td>
</tr>
<tr>
<td>E.g. Playback Errors, Buffering Interval, Google.com latency response time</td>
<td></td>
</tr>
<tr>
<td><strong>Device Identifiers (Mobile Advertiser ID)</strong></td>
<td>Used only according to Digital Advertising Alliance guidelines. Typically used to help wireless service providers and other third parties understand drivers of churn/acquisition, and design effective marketing campaigns.</td>
</tr>
<tr>
<td>Google Advertiser ID or Apple IDFA</td>
<td></td>
</tr>
</tbody>
</table>

Every end user agrees and opts in to sharing this data with Tutela by accepting their mobile application’s permissions and privacy policy. We require that all appropriate consents are granted. Furthermore, our licensing mandates that our application partners provide complete disclosures to end users listing what is collected and how it is used. We audit our application partners regularly to ensure that these requirements are being satisfied.
Where we collect data.

Tutela collects data wherever there is an opportunity to improve wireless networks. We may implement more strict collection and storage practices based on geography to comply with region specific privacy and data protection requirements.

We prevent user identification.

We do not collect any sensitive personal information from users. In fact, our users are completely anonymous to us. We never collect name, email address, phone number, social media ID, contact list, or anything else which directly identifies individuals.

Additionally, we do not use or store a persistent internal device ID. Each device sending us data is assigned a random identification code generated by our software (called a “Tutela ID”), which is used to assign network measurements to the device and create daily aggregate metrics. Our Tutela ID resets every 24 hours to a new random number to help prevent the unlikely possibility of user identification.

We transmit and store data secure from malicious attacks.

We use the latest data security methods and premium data centers to ensure data is held securely. Our data is stored in databases encrypted using 256 bit AES encryption and access requires 2-factor authentication.

When data is transferred from mobile devices to our database, we use 256-bit encryption. We monitor the access to our databases carefully to identify any breach of security.

We collect and store only the data we need for our business. No raw data is stored by Tutela for more than 18 months.

We are transparent about why we collect data and how we will use it.

We use data to help companies improve their wireless networks, to identify and communicate aggregate trends in device and user behavior, understand the drivers of subscriber churn and acquisition, design effective marketing campaigns, and to improve wireless security to further protect the privacy rights of consumers.

Tutela’s documentation, available at https://insights.tutela.com publicly discloses all data we collect, how we collect it, and how it is used. This information disclosure is available to everyone, including our competitors, in the interest of full transparency.
For more detail on the nature of our relationship with mobile applications, including their requirements and our provided documentation, please visit https://www.tutela.com/app-developers

We only share data with trusted companies.

Our data is only shared with companies that agree to our strict privacy and data handling terms, or adhere to their own equivalent privacy terms.

Tutela may share data collected from users of applications running Tutela’s software, including geolocation data and our non-persistent identifiers:

a. **With our customers:** Tutela’s customers are generally Tier 1 wireless service providers. You can learn more about our common solutions at https://www.tutela.com/products.

b. **With our employees:** On a need-to-know basis Tutela allows employees to access data so that we might service our customers or develop products.

c. **With our service providers:** For example, for website and data hosting, or hiring auditors to review and ensure our privacy policies and practices meet the highest standards.

d. **With service providers to our customers:** Our customers may contract with companies to help them derive additional value from Tutela’s products and data.

e. **With our subsidiaries and affiliates:** In 2019 Tutela was acquired by Comlinkdata. Together we are proud to bring together complementary data on consumer experience, network performance, and subscriber behaviour. As a merged company we help the telecoms industry to understand and execute on opportunities to better meet the needs and wants of consumers. https://www.tutela.com/tutela-and-comlinkdata-announcement

f. **With public authorities, such as law enforcement:** If we are legally required to do so or if we need to protect our rights or the rights of third parties.
Data collection will not negatively impact our users.

Providing data to us does not have any negative impact on users or their devices. Data we collect cannot be used to disadvantage our users. Quite the opposite; our data is typically used to improve networks and ensure a better experience for users.

The impact to the device battery and CPU is designed and tested to be so small that it cannot be noticed by the average user (less than 1%). For our mobile application and game partners, the additional file size is less than 1 MB. Tutela does download and upload files to test network performance which may count against user data quotas. We work with our app partners to ensure that this doesn’t exceed levels which are acceptable or generally expected from their app.

Our mobile app partners are anonymous.

Our customers and partners cannot use our data to identify the mobile applications or publishers that our data has been received from. We collect data from hundreds (often thousands) of different mobile applications, and our reports, data, and documentation do not reveal which mobile applications the source data was collected from. We do not publicly disclose our application partners without their permission.

Children’s Privacy.

Our services are not intended for children under the age of 16, and we do not knowingly collect information from children under the age of 16. We require that our mobile application partners agree to not include Tutela’s software in applications that are targeted to children and regularly audit our partners’ applications for violations.

National and State Data Protection Acts.

Tutela and its partners take appropriate measures to ensure compliance with data protection legislation in the countries where they offer their services.
Your rights as a data subject.

GDPR and other forms of legislation provide data subjects with certain legal rights in respect of their personal data.

a. **Right to Access:** the right to obtain from the controller confirmation as to whether or not personal data concerning the data subject are being processed. Please note that Mobile Advertiser IDs are not collected from devices in GDPR participating countries.

b. **Right to Rectification:** the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

c. **Right to Erasure:** the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

d. **Right to Restriction of Processing:** the right to obtain from the controller restriction of processing where certain conditions are satisfied.

e. **Right to Data Portability:** the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

f. **Right to Object:** the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.

f. **Right to Lodge Complaints:** you have the right to lodge a complaint with a supervisory authority or other regulatory agency if you believe that we have violated any of the rights concerning personal data about you. We encourage you to first reach out to us at data.protection.officer@tutela.com so we have an opportunity to address your concerns directly before you do so.

The above legal rights are subject to various conditions and exceptions. We take steps to help ensure that you able to exercise your rights. However, the pseudo-anonymous nature of our data may mean that it is impractical to satisfy certain requests as it is materially difficult or not possible to associate data with your identify. To make a request in accordance with the GDPR, please send an email to data.protection.officer@tutela.com with “GDPR Privacy” in the subject line.
Your rights as a California resident.

The California Consumer Privacy Act provides residents of California with certain legal rights in respect of their personal information.

a. **The Right to Know**: the right to request that a business that collects, sells, and/or discloses for a business purpose personal information about the consumer disclose to the consumer the following: the categories of personal information it has collected, sold, and/or disclosed for a business purpose about that consumer; the categories of sources from which the personal information is collected; the business or commercial purpose for collecting or selling personal information; the specific pieces of personal information the business has collected about that consumer; the categories of third parties to whom the personal information was sold.

b. **The Right to Delete**: the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

c. **The Right to Opt-out**: the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.

d. **The Right to Non-Discrimination**: a business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under the CCPA.

Within the past 12 months Tutela has sold or shared the following categories of personal information: Geolocation, Identifiers (Mobile Advertising IDs)

Within the past 12 months Tutela has disclosed for a business purpose the following categories of personal information: Geolocation, Identifiers (Mobile Advertising IDs)

Your particular jurisdiction may utilize a different definition of Personal Information than is contemplated by the CCPA. For a full list of Tutela’s measurements please visit [https://insights.tutela.com](https://insights.tutela.com)

The above legal rights are subject to various conditions and exceptions. We take steps to help ensure that you able to exercise your rights. However, the pseudo-anonymous nature of our data may mean that it is impractical to satisfy certain requests as it is materially difficult or not possible to associate data with your identify. To make a request in accordance with the California Consumer Privacy Act, please send an email to data.protection.officer@tutela.com with “CCPA Privacy” in the subject line, or call us toll-free at +1 (855) 6-TUTELA.
We make it clear how you can opt out.

Users are made aware that they are participating in the collection of Tutela’s pseudo-anonymous statistics prior to downloading and then using an application. In all cases this is explicit and disclosed in the privacy policy that is available on the download pages of participating applications. We also make use of the standard iOS/Android permission requests for data such as location, and in some cases work with our partners to design custom in-app pop-ups which provide even more in-app detail. The procedure for later opting out is generally found in the application’s privacy policy, terms of service, and/or settings menu. Additional opt-out instructions are detailed below.

Note: In exceptional cases we allow individual users to opt-in to provide additional data to Tutela for advanced service troubleshooting. This involves a secondary in-app pop-up consent request beyond basic permission requests. Data includes things such as; when, where, and why phone calls fail; or providing IP address information. These special troubleshooting cases may include data types which are additional to those listed above – which describe the capabilities of our standard configurations available to all mobile applications.

Tutela Opt-out.

Tutela is unable to collect data without having the end user opt in by accepting application permissions and any other consent configured by our application partners. Procedures are provided to support individuals to opt out at any time, as outlined below and at https://tutela.com/opt-out

Opt-out options.

1. End users may review the privacy policy(s) of an application or a group of applications containing Tutela’s software for application-specific opt-out instructions.

2. End users may at their option specifically opt-out of providing Mobile Advertiser IDs:

   a) Android - You may opt out of personalized app ads via “Settings > Google > Ads” and choosing to Opt out of Ads Personalization.

   b) iOS - You may opt out of targeted advertising by going to “Settings > Privacy > Advertising” and turning on Limit Ad Tracking. Please see additional information from Apple here: https://support.apple.com/en-ca/HT202074

   c) The Digital Advertising Alliance offers a third party opt-out procedure which restricts Tutela’s collection of Mobile Advertiser IDs. Visit: http://youradchoices.com/appchoices
3. End users may at their option restrict an application or a group of applications from collecting location data. No data will be collected by Tutela if location permission is not enabled for that app. Please note that if you do deny or revoke location permissions for an application, certain functionalities of the app that rely on location data to function may be affected.

Android Location Turn-Off

Android (6.0 / Marshmallow and higher) - In order to disable the collection of Precise Location Data on Android, you may turn Location off for the applicable App via “Settings > Apps & notifications > [applicable App] > Permissions > Location”. Then “Deny” Location Access.

iOS Location Turn-Off

In order to disable the collection of Precise Location Data on iOS, you may turn off Location Services for the applicable App via “Settings > Privacy > Location Services”. Then select the applicable app and set the “Share My Location” status to “Never”. Please see additional information from Apple here: https://support.apple.com/en-us/HT203033

4. End users may at their option uninstall and stop using applications which have requested data permissions. Tutela’s software will be uninstalled along with our partner application.

5. In accordance with the California Consumer Privacy Act, if you are a California resident you may contact us with your request to opt out of Tutela data collection by emailing us at data.protection.officer@tutela.com, or calling us toll-free at +1 (855) 6-TUTELA. Please include “CCPA Privacy” in the subject line of your email. If you are a California resident and would like an authorized agent to opt out on your behalf, please inform them to utilize any of opt-out options 1-4 as outlined above.

6. If you are a resident of a GDPR participating country you may contact us with your request to opt out of Tutela data collection by emailing us at data.protection.officer@tutela.com. Please include “GDPR Privacy” in the subject line.
Notes on this Privacy Charter.

From time to time we may update this Privacy Charter. You can tell when changes have been made by referring to the “Last updated” date at the top. Please review this Privacy Charter regularly to ensure that you are aware of any changes.

This document does not encompass or detail Tutela’s handling of internal employee or customer data. Tutela’s employees and customers may provide additional personal information such as names, email addresses, and phone numbers through the regular course of business and Tutela’s non-public facing policies, which are available to those groups, govern the handling of that data.

Data Protection Officer.

Please contact Tutela’s Data Protection Officer with any questions or for GDPR, CCPA, or other privacy legislation supported requests. We ask that you limit these messages to only contain information about you that you are willing to share with Tutela. Responses pertaining to data from your mobile may be limited due to the pseudo-anonymous nature of our data set and the identification limitations that places on Tutela.

data.protection.officer@tutela.com