Privacy Charter

Prepared by

Hunter Macdonald, CEO
Tom Luke, VP Sales, Marketing and Alliances
Anthony Kroeker, VP Engineering Systems & Data Protection Officer
Tutela Technologies Ltd.

Reviewed and approved, on the basis of a Privacy Impact Assessment, by

David H. Flaherty, Ph.D.
Privacy and Information Policy Consultant
David H. Flaherty Inc.

TUTELA

Tutela Privacy Charter

As a company whose livelihood depends on data and its proper treatment, Tutela takes data privacy 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.

We collect data so that we can help companies in the mobile industry better understand their networks, understand trends in user and device behavior on aggregate, design effective marketing campaigns, and research cyber security vulnerabilities. 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.

Where we collect data.

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

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:

Category	Typical Use
Device Characteristics (Example: Device Make, Model, OS Version, Screen Resolution)	Wireless device details are required to identify if specific network issues are limited to a device type.
Location	Required to aggregate and plot network performance on a map to convey network coverage
Connection Details (ex: Service provider Name, Roaming Details, Cell Tower Name)	Used to separate data and results by operator and compare their performance to help with competitive analysis
Connection Quality (ex: Download Speed, Network Latency, Signal Strength)	Used to evaluate the performance of wireless networks
Application Usage (ex: App Name, MB Used)	Required to pinpoint the application and services which are consuming the most network bandwidth and creating congestion
Mobile Advertiser ID	Used only according to digital advertiser alliance guidelines to create marketing campaigns targeted at educating user segments which are underserved by their operator (opt-out procedures below)

Every end user agrees and opts in to sharing this data with us by accepting their mobile application's permissions. We require that they give all appropriate consents. 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.

Why we work with mobile apps and games partners.

Collecting data from millions of devices is difficult. 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.

Identification.

We do not collect any identifiable personal data 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 a user.

Additionally, we do not use or store a persistent internal device or Tutela ID. Our Tutela ID resets every 24 hours to a new random number to help to prevent the unlikely possibility of user identification.

We transmit and store data secured 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 twelve months.

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

We only use data to help companies improve their wireless networks, to identify aggregate trends in device and user behavior, market to users, 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, however it is provided 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, which agree to our strict privacy and data handling terms, or adhere to their own equivalent privacy terms. These are generally Tier 1 wireless service providers.

We make it clear what you can opt-in and opt-out of.

Users are made aware that they are participating in the collection of Tutela's pseudo-anonymous statistics when running an application for the first time and are prompted for consent. The procedure for later opting out is generally found in their application terms of service and/or settings menu.

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; providing IP address information, persistent mobile identifies. 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.

Giving data 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 mobile and WiFi networks to provide 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.

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 over 100 different mobile applications, but 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.

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.

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 also provided to support individuals to opt-out at any time.

Opt-Out Options

1. 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.

2. End users may at their option restrict an application or a group of applications from collecting location data. Tutela's service will not initialize and no data will be collected if location permission is not enabled.

   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 the menu "Settings > Apps > [applicable App] > Permissions > Location". Then turn off the "Location" button.

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 the menu "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

3. In many cases end users can revoke specific permissions previously provided to an application

    a. 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 the menu "Settings > Apps > [applicable App] > Permissions > [Applicable Permission]". Then turn off the "Location" button.

    b. iOS (8.0 and higher) - In order to disable the collection of Precise Location Data on iOS, you may turn off Location Services for the applicable App via the menu "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 specifically opt-out of providing Advertiser ID:

    a. Android – You may opt out of personalized app ads via the "Settings > Google > Personal info & Privacy > Ads > Opt out of Ads Personalization"

    b. iOS – You may limit ad tracking via the "Settings > Privacy > Advertising > Turn on Limit Ad Tracking". Please see additional information from Apple here: https://support.apple.com/en-ca/HT202074

    c. Digital Advertising Alliance offers a third party opt-out procedure, which restricts Tutela's collection of Advertiser ID. Visit: http://youradchoices.com/appchoices

Data Protection Officer.

Please contact Tutela's Data Protection Officer with any questions or for GDPR supported data 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

About David Harris Flaherty

David Flaherty is a specialist in the management of privacy and information policy issues. He served a six-year, non-renewable term as the first Information and Privacy Commissioner for the Province of British Columbia (1993-99).

As a consultant since 1999, Flaherty's services for clients have included strategic advice on the management of privacy issues and of relationships with privacy authorities, privacy advocates, and the general public; conducting overall assessments of privacy compliance (privacy reviews, audits, site visits, knowledge transfer); preparing Privacy Impact Assessments; helping to manage and prevent privacy breaches; and developing on-line privacy training and other privacy risk management tools.

David has been a member of both the External Advisory Committee to the Privacy Commissioner of Canada (from the Committee's inception in 2004 till his resignation in early June, 2014) and the expert external advisory board for the BC Office of the Information and Privacy Commissioner since its inception in January 2011. Since 2000, he has been the Chief External Privacy Advisor to the Canadian Institute for Health Information (CIHI). He has also been a Director of MAXIMUS BC Health Inc. since its inception in 2005 as a service provider to the BC Ministry of Health Services through Health Information B.C.

In June, 2013 the Electronic Privacy Information Centre (EPIC) in Washington, DC honored Flaherty with a Lifetime Achievement Award for his work on privacy protection. In October, 2014 the Privacy and Access Council of Canada named him a Fellow, Access and Privacy Professional. In 2017 the University of Victoria conferred on him an honorary Doctorate of Laws.