Privacy

The Privacy Assessment focused on analyzing how current privacy practices in the operation of the LinkNYC system compare to privacy practice requirements found in the LinkNYC Franchise Agreement, privacy policy, and any subsequent amendments to these documents. The findings that resulted from the privacy assessment were organized into six (6) key categories covered by the LinkNYC Franchise Agreement.

The following findings are further elaborated in the Privacy Detailed Findings section of this report.

Category	Finding	Finding
PII Collection/ Gathering	PII collected by CityBridge from LinkNYC users does not exceed what is permitted by the Franchise Agreement.	N/A
PII Sharing	There was no evidence that CityBridge shares PII with third parties or the City beyond what is permitted by the Franchise Agreement.	N/A
PII Data Protection	Other than the use of encryption versus anonymization of PII, no other significant gaps were identified in how PII collected from LinkNYC users is protected by CityBridge.	PF-01
PII Retention	PII collected through the LinkNYC system (i.e., the user email address) appears to be purged within 12 months as outlined in the Franchise Agreement.	N/A
Consent Management	CityBridge appears to follow the consent management requirements set out in the Franchise Agreement although some inconsistencies regarding the privacy policy version and language displayed to LinkNYC users were observed during fieldwork.	PF-02
Communications	Testing procedures revealed that current communications practices limit the ability of LinkNYC users to choose what communications they would like to receive.	PF-03 PF-04

Finding	Description	CityBridge Remediation Plan
PF-01	**CityBridge does not anonymize the MAC Address of user devices as stated in the Privacy Policy and Franchise Agreement.**	CityBridge indicated that two years ago it began to transition the LinkNYC wireless access gateway from Google to Global Reach and this transition resulted in the MAC addresses only being encrypted and not anonymized. CityBridge has discussed a solution with Global Reach and ZenFi and the hashing of MAC addresses will be rolled out to production by March 31, 2022.
PF-02	**Users of the LinkNYC system are provided an Intersection privacy policy vs. LinkNYC privacy policy.**	CityBridge indicated the display of the Intersection Privacy Policy instead of the LinkNYC privacy policy was attributed to a bug in the Global Reach system. CityBridge confirmed that changes have been pushed to the LinkNYC kiosks so that the captive portal displays the correct privacy policy. CityBridge will provide QC documentation to the assessment team as confirmation of the change being made and conduct a root cause investigation to determine how long the Intersection privacy policy has been displayed to LinkNYC users and which location(s) were impacted.
PF-03	**LinkNYC welcome emails do not consistently include the required "unsubscribe" option on some test devices as per the CityBridge privacy policy.**	CityBridge confirmed that the LinkNYC Welcome email has been updated to include an unsubscribe link and was live on the system as of November 12, 2021.

Finding	Description	CityBridge Remediation Plan
PF-04	**Gap in required information to be displayed on the Splash Page.**	CityBridge indicated that it will direct its Wi-Fi services provider to update the Captive Portal to present the correct version of the LinkNYC Terms of Service. The timeline for this transition is March 31, 2022.

Privacy Assessment Summary

Overview of Privacy Assessment Results

As described in the **Approach Overview** section earlier in this report, the Privacy APG contained a total of thirty-four (34) controls based off requirements established in LinkNYC Franchise Agreement and Privacy Policy. The assessment team collected documents, conducted interviews with CityBridge and other third-party vendors, and conducted in person testing activities to evaluate the APG controls.

The table below provides a summary of all Privacy APG controls identified by a unique reference (e.g., P-01 = Privacy APG #1], and whether the evaluation of the control resulted in one of the following:

APG Result	Description
Finding	Negative observation or gaps were identified with respect to Franchise the Agreement based on test procedures outlined in the APG.
No finding	No negative observation or gaps identified with respect to the Franchise Agreement based on test procedures outlined in the APG.
Not testable	Unable to test or evaluate performance against the Franchise Agreement term due to: — Service or feature not being required and not installed by CityBridge — An event not occurring that would allow for the control to be tested

Where the evaluation of a control did not result in a finding or could not be evaluated, the specific procedures performed to test that control and the result can be found in the Privacy APG (See **Appendix A)**. Where the evaluation of a control in the APG resulted in a finding, the finding is assigned a unique identifier (e.g., PF-01) and additional details to support the finding are documented in the APG and the following section.

APG #	Contractual Document/Section	Finding/Result
P-01	**City Bridge Privacy Policy - Information Collection**	**PF-01**
P-02	City Bridge Privacy Policy - MAC Address Collection and Management	No finding
P-03	City Bridge Privacy Policy - Technical Information Collection	No finding
P-04	City Bridge Privacy Policy - Location Information	No finding
P-05	City Bridge Privacy Policy - Payment Information	No finding
P-06	City Bridge Privacy Policy - Do Not Track Feature	No finding
P-07	**City Bridge Privacy Policy - Your Choices**	**PF-03**
P-08	City Bridge Privacy Policy - How Your Information is Used	No finding
P-09	City Bridge Privacy Policy - Information Analytics	No finding
P-10	City Bridge Privacy Policy - Opt-In Consent Information Use	No finding
P-11	City Bridge Privacy Policy - Sharing and Selling of PII	No finding
P-12	City Bridge Privacy Policy - Service Providers and Subcontractors	No finding
P-13	City Bridge Privacy Policy - Information Sharing with NYC Open Data	No finding
P-14	Franchise Agreement - Section 3.12.1 - Ownership Rights in CityBridge Data	No finding
P-15	Franchise Agreement - Section 3.12.3 - Protecting Confidential Data	Not testable – event did not occur
P-16	Franchise Agreement - Section 3.12.4 - Disclosure of City Data	Not testable – event did not occur
P-17	Amendment No. 1 - Section 3.12 - Ownership Rights in CityBridge Data	No finding
P-18	Amendment No. 1 - Section 3.12.15 - License to Use Anonymized Data	No finding
P-19	City Bridge Privacy Policy - Disclosures Required by Law	Not testable – event did not occur
P-20	City Bridge Privacy Policy - Retention and Securing of PII	No finding
P-21	City Bridge Privacy Policy - Environmental Sensors	Not testable – feature not required or installed
P-22	City Bridge Privacy Policy - Cameras and Recording	No finding
P-23	City Bridge Privacy Policy - USB Ports for Charging Devices	No finding
P-24	City Bridge Privacy Policy - Services Not Intended to Knowingly Target Children	No finding
P-25	City Bridge Privacy Policy - Email Address Management	No finding
P-26	Exhibit 1 Minimum Terms of Service - Terms of Service	No finding
P-27	Attachment SRV - Section 4.4.1 - Splash Page Requirements	No finding
P-28	**Attachment SRV- Section 4.4.2 - Splash Page Responsibilities**	**PF-04**
P-29	Attachment SRV - Section 4.4.3 - Splash Page Advertising Revenue	No finding
P-30	**Attachment SRV- Section 4.4.4 (i) - Splash Page - Disclosing PII**	**PF-01**
P-31	Attachment SRV - Section 4.4.4 (ii) - Splash Page Disclosure Required by Law	Not testable – event did not occur
P-32	**Attachment SRV- Section 4.4.4(iv) - Splash Page Link to Wi-Fi Privacy Policy**	**PF-02**
P-33	Attachment SRV - Section 4.4.4(v) - Splash Page Privacy Policy Revisions	No finding
P-34	Attachment SRV - Section 4.4.4(vi) - Splash Page Privacy Policy Compliance	No finding

Detailed Findings and Recommendations

Below are the detailed finding and recommendations that were identified from this privacy assessment.

PF-01: CityBridge does not anonymize the MAC Address of user devices as stated in the Privacy Policy.	
Observations	In the CityBridge Franchise Agreement, Privacy Policy - Section 2 - Information Collection, it states *"We collect certain information to help us operate and provide the Services to you. We collect this "Technical Information" when you use the Services, including: 1. MAC address **(anonymized)**, IP address, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, device type, and device identifiers; 2. Information about your visits…"* Through interviews and testing, it was determined that this requirement is not implemented as written in the Franchise Agreement. As stated above, since the inception of the LinkNYC program in approximately 2014, MAC Addresses were anonymized, in line with Franchise Agreement requirements. When these documents were written, Global Reach, the vendor managing the captive portal, was using Google as their infrastructure vendor. Google anonymized user MAC (device hardware) addresses using a hash algorithm (unreadable format) meaning that the data could not be associated back to an individual. In approximately June of 2021 when Global Reach changed the infrastructure vendor from Google to ZenFi, the updated solution only protects the data via encryption of the MAC Addresses. The assessment team also tested this by creating test data (Device type, MAC Address and Email ID) in multiple kiosks by connecting to the LinkNYC Wi-Fi services using mobile devices and laptops. The Technical Information (MAC Address) is stored in a MongoDB database managed by Global Reach. Global Reach provided a live demonstaration and supporting screenshots of the testing devices and the correspoding MAC Address data in MongoDB. After review, it was noted that the MAC Address was not anonymized, but instead stored on disks which are encrypted at rest. As such, the MAC Address is not being anonymized using a hash algorithm as indicated in the Franchise Agreement.
APG Reference(s)	P-01, P-30
Risks	The risk with using an encrypted disk without anonymization is that the user's personal information (MAC Address) can be decrypted and presented in plain text to anyone with access to the key in AWS Key Management Services (KMS). As a result, anyone that has the access to the decryption key can decrypt the data and access LinkNYC user information that is being collected and stored. Since the inception of the LinkNYC program in approximately 2014, MAC Addresses were anonymized, in line with Franchise Agreement requirements. When these documents were written, Global Reach was using Google as their infrastructure vendor. Google anonymized user MAC (device hardware) addresses using a hash algorithm (unreadable format) meaning that the data could not be associated back to an individual. In approximately June of 2021 when the vendor managing the captive portal was changed by Global Reach from Google to ZenFi, the updated solution only protects the data via encryption of the MAC Addresses. While both approaches are generally sound

	and commonly used in industry, anonymization is generally better as it removes any ability to identify the original MAC Address, whereas encryption protects it, but a limited set of individuals from CityBridge, Global Reach or ZenFi with a decryption key could decrypt to identify the original MAC Address. As the Franchise agreement is currently written, the LinkNYC solution has not been compliant since approximately June 2021.
Recommendations	
The assessment team recommends that Global Reach anonymize the MAC address using a hash algorithm for enhanced security.	
Evidence	
See **Appendix D** – Figure 1.0, Figure 2.0	
CityBridge Response 12/17/2021	
CityBridge indicated that two years ago it began to transition the LinkNYC wireless access gateway from Google to Global Reach and this transition resulted in the MAC addresses only being encrypted and not anonymized. CityBridge has discussed a solution with Global Reach and ZenFi and the hashing of MAC addresses will be rolled out to production by March 31, 2022.	

CityBridge Response 12/23/2021

Agree to Remediate?	Plans for Remediation	Planned Completion
Yes	The CityBridge team has instructed our Wi-Fi services vendor to implement a hashed MAC solution for the collection of user MAC addresses and upon completion of this work any unhashed MAC addresses will be expunged.	March 31, 2022
CityBridge Comments	MAC addresses are required to enable a device to connect to our network and are only used to provide Wi-Fi services. MAC addresses are only retained to enable a user to automatically reconnect to the network. From the inception of the program, CityBridge's Wi-Fi services vendor utilized a network solution that hashed users MAC addresses to ensure anonymity. In 2020, CityBridge's Wi-Fi services vendor began to transition certain aspects of the network solution that resulted in storing MAC addresses securely but not hashed. This transition occurred over a period of multiple months with Staten Island devices being the first group to transition on May 26, 2020 followed by Queens on June 1, 2020, Brooklyn on June 2, 2020, the Bronx on July 6, 2020, and finally Manhattan on July 8, 2020.	

PF-02: Users of the LinkNYC system are provided an Intersection privacy policy rather than the LinkNYC privacy policy.	
Observations	The assessment team conducted physical testing of the LinkNYC kiosks across the City with a variety of devices. When connecting to the LinkNYC public wi-fi network a user is prompted to view the LinkNYC Privacy Policy and Terms of Serivce. Through these testing activities, it was observed in all instances that when clicking the link to view the

	Privacy Policy, the user is directed to the Intersection Privacy Policy instead of a LinkNYC Privacy Policy.
APG Reference(s)	P-32
Risks	The display of an incorrect Privacy Policy to users who are sharing PII (i.e., their email address) and accessing Wi-Fi servers is informing users of potential inconsistent processes, information, and requirements with how their information is being handled, stored, and shared upon connection to the LinkNYC Wi-Fi network.

Recommendations

The assessment team recommends that CityBridge change the Privacy Policy link on the LinkNYC Splash Page to display the LinkNYC Privacy Policy instead of the Intersection Privacy Policy.

Evidence

See **Appendix D**– Figure 4.0

CityBridge Response 12/17/2021

CityBridge indicated the display of the Intersection Privacy Policy instead of the LinkNYC privacy policy was attributed to a bug in the Global Reach system. CityBridge confirmed that changes have been pushed to the LinkNYC kiosks so that the captive portal displays the correct privacy policy. CityBridge will provide QC documentation to the assessment team as confirmation of the change being made and conduct a root cause investigation to determine how long the Intersection privacy policy has been displayed to LinkNYC users and which location(s) were impacted.

CityBridge Response 12/23/2021

Agree to Remediate?	Plans for Remediation	Planned Completion
Yes	CityBridge's Wi-Fi service provider deployed the correct LinkNYC Privacy Policy on November 11, 2021. CityBridge deployed field technicians to test and verify successful deployment on November 12, 2021. This field testing was successful.	November 11, 2021
CityBridge Comments	CityBridge's Wi-Fi service provider transitioned certain services over the course of 2020. Specifically, Staten Island devices were the first group to transition in May 26, 2020 followed by Queens on June 1, 2020, Brooklyn on June 2, 2020, the Bronx on July 6, 2020, and finally Manhattan on July 8, 2020. As a result of the transition of one of those services, a 'bug' was introduced into the software codebase that delivered the Privacy Policy via the Captive Portal. This error resulted in the occasional and random presentation of the incorrect Privacy Policy via the Captive Portal to Wi-Fi users.	

PF-03: LinkNYC welcome emails do not consistently include the required "unsubscribe" option on some test devices.	
Observations	The CityBridge Franchise Agreement, Privacy Policy - Section 9 - Your Choices states, *"When you register with us, you may choose to receive certain communications from us related to the Services.* ***You can update your communications choice at any time by clicking "unsubscribe"*** *at the bottom of these emails…"* The assessment team connected to LinkNYC Kiosks with multiple devices and registered with different email addresses. Only six (6) out of ten (10) devices received a welcome email and the welcome email was sent without an "unsubscribe" option as indicated in the Privacy Policy. Additionally, when a user registers at the kiosk there is no email validation controls in place to ensure that the user is providing a valid email address. The 4 devices that connected to the kiosk and did not receive a welcome email are as follows: 1. iPhoneX 2. iPhoneXR 3. iPad 4. Samsung tablet
APG Reference(s)	P-07
Risks	Users not receiving a welcome email and not giving users an option to unsubscribe is a violation of the LinkNYC Privacy Policy. In the Privacy Policy, it states that users will have the option to unsubscribe to CityBridge emails.
Recommendations	
It is recommended that CityBridge have all necessary controls in place to send devices welcome emails to users when connecting to the LinkNYC Wi-Fi network. Additionally, CityBridge needs to add an unsubscribe link to all email communications giving users the option to opt-out of receiving emails from CityBridge, which is legally mandated to protect user rights around which communications they receive when signing up for services.	
Evidence	
See **Appendix D** – Figure 3.0	
CityBridge Response 12/17/2021	
CityBridge confirmed that the LinkNYC Welcome email has been updated to include an unsubscribe link and was live on the system as of November 12, 2021.	
CityBridge Response 12/23/2021	

Agree to Remediate?	Plans for Remediation	Planned Completion
Yes	CityBridge has updated the welcome email to include an unsubscribe link as of November 12, 2021. An artifact	November 11, 2021

	demonstrating this update was shared with the [Assessment Team] on November 12, 2021.	
CityBridge Comments	It is important to note that, as CityBridge previously indicated, the Privacy Policy states that users may choose to receive certain communications from CityBridge related to Services and that (if and only if such users have chosen to received such communications) those same users may update their communications choice at any time by choosing to "unsubscribe." To date, CityBridge has not provided the option to users to receive certain communications related to Services and the welcome email was and remains in compliance with the Privacy Policy.	

PF-04: Gap in required information to be displayed on the Splash Page	
Observations	Section 4.4.2 of the Attachment SRV (Services) to the LinkNYC Franchise Agreement states that, *"The Franchisee shall include on the Splash Page(s) terms of service substantially reflecting the provisions of Exhibit 1, including a statement in a form satisfactory to DoITT which in substance informs Users that the City of New York is not responsible for any material that may subsequently be presented or received by means of the Wi-Fi Service…"* The assessment team conducted fieldwork on October 11, 2021 connecting various devices (iPhone X, Android tablet, iPad, laptop, etc.) to kiosks around New York City. When the assessment team's devices were connecting to the LinkNYC network, a splash page was shown. The splash page prompts the user to insert their email address and contains links to the Privacy Policy and the Terms of Use. However, does not include a statement that is mentioned in the Attachment SRV that should be displayed stating that "the City of New York is not responsible for any material that may subsequently be presented or received by means of the Wi-Fi Service."
APG Reference(s)	P-28
Risks	Without the statement included on the Splash Page, users could interpret that the City of New York is responsible for providing the LinkNYC services.

Recommendations

The assessment team recommends including all necessary and appropriate information contractually agreed upon to be displayed to the users on the Splash Page when connecting to the LinkNYC network.

CityBridge Response 12/17/2021

CityBridge indicated it did not have a response and would take the finding under review.

CityBridge Response 12/23/2021

Agree to Remediate?	Plans for Remediation	Planned Completion
Yes	CityBridge will direct its Wi-Fi services provider to update the Captive Portal to present the correct version of the LinkNYC Terms of Service. The timeline for this transition is outlined on Slide 1 [PF-1].	March 31, 2022

CityBridge Comments	The previous Terms of Service was compliant with 4.4.2 of attachment SRV of the LinkNYC franchise agreement, however, the incorrect Terms of Service was incorporated as part of the 2020 network transition. Requirement 4.4.2 of Attachment SRV of the LinkNYC franchise agreement indicates that CityBridge "shall include on the Splash Page(s) terms of services substantially reflecting the provisions of Exhibit 1, including a statement in a form satisfactory to DoITT which in substance informs Users that the City of New York is not responsible for any material that may subsequently be presented or received by means of the Wi-Fi Service." The CityBridge splash page provides a link to the Terms of Service and Privacy Policy (all shared previously to [Assessment Team]). The Terms of Service linked to from this Splash page has historically included Limitation of Liability and Parental Controls provisions that indicates neither the City nor CityBridge are responsible for any material presented or received via the Wi-Fi Service. Through an investigation of this issue, however, CityBridge became aware that the link.nyc website Terms of Use is being presented to the Wi-Fi user via the Splash page rather than the Wi-Fi Terms of Service. In 2020, CityBridge's Wi-Fi services vendor began to transition certain aspects of the network solution that resulted in the incorrect Terms of Service being offered. This transition occurred over a period of multiple months with Staten Island devices being the first group to transition in May 26, 2020 followed by Queens on June 1, 2020, Brooklyn on June 2, 2020, the Bronx on July 6, 2020, and finally Manhattan on July 8, 2020.

LinkNYC Vendor and Data Privacy Landscape

The LinkNYC Franchise Agreement authorizes CityBridge to install, operate, and maintain the LinkNYC system. However, through the assessment team's meetings with CityBridge and review of CityBridge documentation it was revealed that several aspects of the LinkNYC system and operations are contracted out by CityBridge to third-party vendors placing CityBridge in a vendor oversight role rather than a direct service provider. As such, to understand the privacy practices of the LinkNYC environment involves understanding the network of CityBridge's vendors involved and their respective roles. Below is an overview of the vendors contracted by CityBridge to operate the LinkNYC system, the vendor's role, and what PII they collect from LinkNYC users.

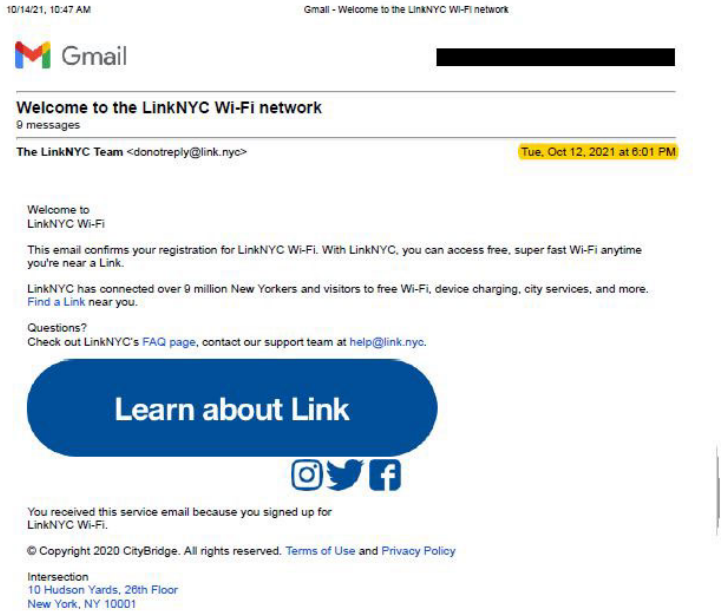
Vendor	Vendor Role	PII/Technical Information
Zendesk	Provides customer support ticketing services to CityBridge.	– Username – User email – User phone number – Additional details provided by the user in the support ticket
Global Reach	Operates the network authentication services and the captive portal - the web page that LinkNYC users can access and provide their email to sign up for LinkNYC Wi-Fi services.	– MAC address (Media Access Control) – Session data (i.e., the time that a user is connected to the LinkNYC system) – Encrypted user email addresses
ZenFi Networks	Operates the LinkNYC network infrastructure. (Previously Google or Alphabet since inception in 2014, until approximately June 2021).	– MAC address
Datadog	Monitors the physical condition of the kiosks.	– No PII collected
Iron Mountain	Provides escrow software services, where they securely maintain source code of the LinkNYC system.	– No PII collected
Sitetracker	Provides software tool used for workflow and project management of tracking the installation and maintenance of LinkNYC kiosks.	– No PII collected
Amazon Web Services (AWS)	Provides cloud hosting services secured in the AWS environment.	– User email addresses – Camera footage
Purple Communications	Provides video relay service that allows the hearing impaired to connect with a live person for kiosk and call assistance.	– Camera footage – User phone numbers
Ring Central	Facilitates calls made from the PCS.	– User phone numbers
Intersection	Supports all aspects of the advertising displayed on the LinkNYC kiosks.	– No PII collected

Appendix D – Privacy Supporting Artifacts

Figure 1.0: The image below is a screenshot capture of the Global Reach Database log showing the Technical Information captured from a LinkNYC user.

Figure 2.0: The image below is a screenshot capture of the Global Reach Database log showing the Technical Information captured from a LinkNYC user.

Figure 3.0: The image below reflects an example of a welcome email received from CityBridge after test devices connected to Wi-Fi from a LinkNYC kiosk and registered. There is no reference to an unsubscribe option.



10/14/21, 10:47 AM Gmail - Welcome to the LinkNYC Wi-Fi network

Gmail [redacted]

Welcome to the LinkNYC Wi-Fi network

9 messages

The LinkNYC Team <donotreply@link.nyc> Tue, Oct 12, 2021 at 6:01 PM

Welcome to
LinkNYC Wi-Fi

This email confirms your registration for LinkNYC Wi-Fi. With LinkNYC, you can access free, super fast Wi-Fi anytime you're near a Link.

LinkNYC has connected over 9 million New Yorkers and visitors to free Wi-Fi, device charging, city services, and more.
Find a Link near you.

Questions?
Check out LinkNYC's FAQ page, contact our support team at help@link.nyc.

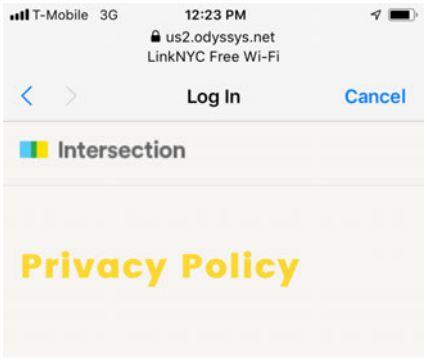
Learn about Link

You received this service email because you signed up for
LinkNYC Wi-Fi.

© Copyright 2020 CityBridge. All rights reserved. Terms of Use and Privacy Policy

Intersection
10 Hudson Yards, 26th Floor
New York, NY 10001

Figure #4.0
The image below is a screenshot of the Intersection Privacy Policy that is displayed upon connection to the LinkNYC public wi-fi network. This was captured during the assessment team's in person testing procedures.



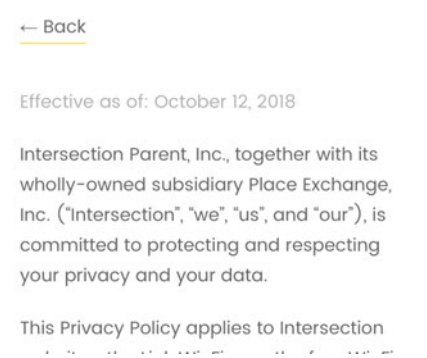
T-Mobile 3G 12:23 PM

us2.odyssys.net
LinkNYC Free Wi-Fi

Log In Cancel

Intersection

Privacy Policy



← Back

Effective as of: October 12, 2018

Intersection Parent, Inc., together with its wholly-owned subsidiary Place Exchange, Inc. ("Intersection", "we", "us", and "our"), is committed to protecting and respecting your privacy and your data.

This Privacy Policy applies to Intersection

Figure #5.0
Below is an image of the LinkNYC splash page collected by the assessment team on November 1, 2021.