

The Stop LinkNYC Wi-Fi & Advertising Network Primer

How Alphabet and the City of New York's LinkNYC Monopoly Wi-Fi Network Harms Internet Access and Web Competition, Invades Privacy and Tracks People, Violates Constitutional Rights, and Pollutes New York City's Environmental Aesthetics

**Authored By:
The Stop LinkNYC Coalition
March 2019**
(Original Version, October 2017)

Preface

This document advocates for the removal of Alphabet and the City of New York's LinkNYC Wi-Fi and Advertising Network in New York City due to monopoly, privacy, constitutional, and quality of life issues.

It encourages Federal and State authorities, as well as the Media, to investigate various aspects around how the Wi-Fi and Advertising franchise was awarded by the City of New York as well as the potential financial and economic harm Alphabet and the City of New York's monopoly Wi-Fi public-private partnership could have on wireline, wireless, and Web services market segments.

Distribution List Information

In October 2017, this document was sent to 400 individuals in the organizations listed below as an electronic file on a USB drive via the United States Postal Service.

New York City Council Members
New York City Franchise and Concession Committee
New York City Borough Presidents
New York City Executive Offices
Manhattan Community Boards
New York State Executive Offices
New York State Legislative Committees
New York State Assembly and Senate Members
Federal Government Executive Offices
Federal Government Legislative Committees
Federal Government House and Senate Members
Privacy Groups
Policy Groups
Law Firms
Media
Wireline and Wireless Communications Companies
Investment Bank Financial Analysts

Table of Contents

<p>Overview of Issues with the LinkNYC Wi-Fi & Advertising Network Quick overview of issues associated with the LinkNYC Wi-Fi & Advertising Network.</p>	<p>5</p>
<p>Summary of Issues Summarizes some of the main issues with the LinkNYC Wi-Fi & Advertising Network, including the: negative environmental aesthetics of the units and electronic ads; negative physical and mental health aspects of electronic ads; the threats to privacy, tracking, surveillance, and Constitutional rights; illegal capabilities included in the Wi-Fi units; the Wi-Fi monopoly threat to wireless and wireline markets as well as the monopolistic financial and other benefits to Alphabet (Sidewalk/Intersection) and the City of New York; the discriminatory and illegal Wi-Fi unit geographic deployment strategy; possible ethics and corruption issues in awarding the franchise; and more.</p>	<p>6 - 8</p>
<p>Background on Corporate Structure of Alphabet/Sidewalk/Intersection/CityBridge Reviews the company’s corporate structure as well as its digital advertising revenue generation model and why it wants to collect metadata, personal data, and geo-location data for mobile and home Internet devices.</p>	<p>9- 10</p>
<p>Terminology and Definitions Provides explanations for words, phrases, technologies, and acronyms.</p>	<p>11 - 14</p>
<p>Negative Quality of Life Issues Discusses how LinkNYC Wi-Fi units negatively affect the quality of life in New York City, including: advertising rotation scheme; size of Wi-Fi units; bright colors and complex graphics used in electronic ads; physical/mental health issues of electronic ads; inclusion of illegal capabilities in the Wi-Fi units; government messages displayed to the public; use of the units as entertainment platforms; the low minimum franchise fee used to justify the Wi-Fi network; the potential monopolistic benefits to Alphabet and the City of New York; the discriminatory/illegal Wi-Fi unit geographic deployment strategy; and more.</p>	<p>15 - 29</p>
<p>Privacy, Tracking, Surveillance, and Constitutional Rights Issues Discusses the threats LinkNYC Wi-Fi poses to privacy and Constitutional rights; what MAC Addressing and Packet Sniffing are and how Alphabet (Sidewalk/Intersection) and the City of New York could use them to personally identify and track people; surveillance and privacy violations via the Wi-Fi units’ cameras and audio capabilities; the illegality of non-Wi-Fi capabilities included in the units; examples of how pedestrians, motorists, bicyclists, and minors can be tracked down to the block, 24/7/365; the difference between a user and non-user of LinkNYC and how each of their privacy rights can be violated; how Alphabet (Sidewalk/Intersection) and the City of New York can generate revenue by violating people’s privacy; Alphabet’s ineffective privacy policy; issues with the Beta Test; the fuzzy claim that “over 25% of New Yorkers lack high-speed broadband service”; Constitutional rights issues; the potential monopolistic financial benefit to Alphabet and the City of New York; and more.</p>	<p>30 - 77</p>
<p>Health and Transportation Issues Raises potential health issues of the LinkNYC Wi-Fi units to adults, children, toddlers, and babies. Discusses how the network could be used beyond its legal limitations as defined in the Franchise Agreement for license plate recording, tracking of motorists, and transportation-related issues and objectives that were not used by the City for justifying or approving the Wi-Fi network.</p>	<p>78 - 81</p>
<p>Monopoly and Anti-Competition Issues Discusses how the public-private partnership between Alphabet (Sidewalk/Intersection) and the City of New York creates a monopoly Wi-Fi service that may negatively impact existing wireline and wireless broadband providers, including: how the monopoly can price Wi-Fi Internet access below the equilibrium price set by the competitive market; the monopolistic financial benefit to both Alphabet (Sidewalk/Intersection) and the City; the market dominance Alphabet possesses in mobile device operating systems as defined by the Herfindahl-Hirschman Index and how it can be used to violate privacy; the potential loss of government taxes/fees; the loss of employment in existing wireless and wireline companies; why Alphabet and the City would want to harm and decimate the existing market for broadband service; the monopolistic benefit to Alphabet of capturing device metadata through the Wi-Fi network; how Alphabet could cross-subsidize the monopoly Wi-Fi service with revenue from its Web businesses to the detriment of existing wireless, wireline, and Web market participants; and more.</p>	<p>82 - 95</p>
<p>Ethics and Corruption Issues Discusses Alphabet and the City’s fuzzy claim that “over 25% of New Yorkers lack high-speed broadband service”; the discriminatory and illegal Wi-Fi unit geographic deployment strategy; the monopolistic financial benefit of the LinkNYC Wi-Fi network to the City and Alphabet; the potential ethical and legal violations by former City of New York employees who may have been involved in awarding or influencing the award of the Wi-Fi and advertising franchise to Sidewalk/Intersection/CityBridge and who also later became high level executives of the company.</p>	<p>96 - 106</p>
<p>Conclusions, Recommendations and Appendix</p>	<p>107 -108</p>

Overview of Issues with LinkNYC Electronic Billboard Kiosks

The City of New York (the City) and the company Alphabet/Sidewalk/Intersection have created a public-private business venture to display electronic advertisements that will fund free Wi-Fi broadband service through 10,000 Electronic Billboard Kiosks (EBKs) branded as LinkNYC. These electronic advertising and Wi-Fi units are to be deployed on virtually every block of Manhattan and many other blocks of the other four boroughs of New York City. This new public-private partnership (PPP) is the first of its kind to be done in America on such a massive scale and raises serious issues regarding:

- 1) The negative impact on the quality of life to residents of New York City, including their mental and physical well-being.
- 2) The negative impact on the environmental aesthetics of New York City and, in particular, of residential areas and mixed residential/commercial areas.
- 3) The government and politically-oriented communications the City wants to have with its residents.
- 4) The privacy of both users and non-users of the LinkNYC Wi-Fi units with respect to its wireless access functionality capturing mobile device MAC Addresses, which can be used to locate and track people throughout New York City down to the block or building, 24/7/365.
- 5) The privacy and tracking of people through the recognition, recording, and analysis of faces/images/conversations captured by LinkNYC's video, audio, and audio sensing capabilities.
- 6) The privacy of individuals in their domiciles due to LinkNYC video cameras directed towards their windows.
- 7) The threat to peoples' civil rights under the 1st, 4th, 5th, 9th, and 14th Amendments to the Federal Constitution.
- 8) The privacy of users and non-users with respect to their personal relationships and personal activities.
- 9) The threat the LinkNYC public-private Wi-Fi monopoly poses to the viability of the competitive marketplace for Internet and broadband services provided by wireless, wireline, and Web services companies.
- 10) The massive financial benefit to Alphabet and the City of New York that could be gained by the LinkNYC network siphoning customers away from existing wireless, wireline, and Web services due to its a) monopoly status and b) ability to provide broadband Internet Wi-Fi service below the equilibrium price set by the competitive market.
- 11) The threat of reduced tax revenues from existing fee-for-service wireless and wireline broadband providers due to loss of business to the free Wi-Fi service offered by the monopoly partnership.
- 12) The legal violations of the Franchise Agreement, by Alphabet and the City of New York, through the inclusion of video, audio, and photographic recording and sensing capabilities in the units, as well as the inclusion of a Web browser.
- 13) The discriminatory and possibly illegal geographic deployment strategy of the Wi-Fi units, where one Borough – Manhattan – receives over 50% of the required structures.
- 14) The ethics and legality of how the LinkNYC Electronic Billboard Kiosk contract was awarded.
- 15) The potential ethical and legal violations of public and private sector personnel who were involved in creating, approving, and awarding the franchise.

Because of the extremely serious and numerous issues raised by the LinkNYC Electronic Billboard Kiosks (EBKs), this document has been sent to individuals in both the public and private sectors, including: U.S. Department of Justice's Anti-Trust and Civil Rights Divisions; U.S. Department of Transportation; U.S. Department of Commerce; OSHA; Federal Communications Commission; Federal Trade Commission; Securities and Exchange Commission; civil rights and privacy rights organizations; consumer watchdog groups; various executive departments within the City and State of New York (including the DOT, DoIT, Corporation Counsel, Attorney General's Office, Franchise Concession and Review Committee, Public Advocate, and others); New York City Council; New York City Community Boards; New York State Assembly; New York State Senate; Congressional Committees; House and Senate Members; print, broadcast, cable and Web media companies; public policy institutions and think tanks; wireless and wireline companies; and investment bank financial analysts.

Summary of LinkNYC Electronic Billboard Kiosks Issues

This section summarizes the major issues raised by the LinkNYC Electronic Billboard Kiosks (EBKs) in New York City. Other important issues not included in this summary section, but which are related to these areas of concern, are explored in the relevant sections of the document as well. The term Electronic Billboard Kiosk, or EBK, is used in this document because it better describes the dual nature of LinkNYC, which is to provide Wi-Fi service and display digital ads on the units' electronic billboards.

EBK Electronic Advertisements Impact the Quality of Life of New Yorkers

The EBKs raise serious quality of life issues for New York City residents due to the Times Square-ification of virtually every block of Manhattan and many other blocks of the other four boroughs. The size, color, content, and rotation frequency of the advertisements are distracting and disturbing. The extremely large size and high number of EBK units is also distracting and disturbing. All of these negative attributes force people to look at the electronic advertisements as they walk down the street; it is difficult to look straight ahead because the EBK form factor and electronic advertising scheme are designed to force you to look at them, resulting in constant eye and head turning. In addition, the EBK form factor design, height, and advertisements are ugly and create a dissonance in the visual environmental aesthetics of both residential areas and minor commercial districts.

EBK Wi-Fi Capability on Virtually Every Block Raises Major Privacy Issues for Users and Non-Users

Because of the underlying technical standard that governs how Wi-Fi operates, the EBK Wi-Fi service will capture everyone's unique mobile device identification number (the MAC Address) for those who have Wi-Fi enabled (that is, turned on in their device's Settings screen). So, regardless of whether an individual has logged into the EBK Wi-Fi service, the units will capture the unique identification numbers of all mobile devices in New York City. This creates numerous privacy situations, as outlined below. Importantly, Alphabet/Sidewalk/Intersection can run analytic software programs to personally identify individuals from only "anonymous" unique mobile device data its EBKs capture.

Major privacy issues related to the unique device IDs (MAC Addresses) captured from mobile phones, other mobile devices, home computers, and other Internet-capable products by the LinkNYC Electronic Billboard Kiosks (EBKs) include:

- 1) **The ability of the City of New York and Alphabet/Sidewalk/Intersection to know the *discrete physical location* of a device, non-user, or user down to the block or building everywhere in New York City where EBKs are located, 24 hours a day, 7 days a week, 365 days a year (24/7/365).**
- 2) **The ability of Alphabet to *track* devices, non-users, and users throughout New York City down to the block or building, 24/7/365.**
- 3) **The ability of the City and Alphabet/Sidewalk/Intersection to *derive personally identifiable information from only the "anonymous" unique device ID (MAC Address) captured by EBKs.***
- 4) **The ability of Alphabet to *sell or provide to private companies and government entities the location and tracking data of mobile devices for both non-users and users of EBK Wi-Fi service.***
- 5) **The ability of Alphabet to *determine personal relationships from mobile devices moving in tandem with each other.***
- 6) **The ability of Alphabet to *determine personal relationships through pattern recognition analytics.***
- 7) **The ability of Alphabet to *track motorists/passengers driving in the city who have either a) their mobile device's Wi-Fi enabled and/or b) on-board vehicle Wi-Fi enabled.***

The Stop LinkNYC Primer

EBK Video, Audio, and Image Recording Capabilities on Virtually Every Block Raise Serious Privacy Issues

The EBKs contain video, audio, and image recording capabilities. Not even considering the legality of having these technologies embedded into the units pursuant to the terms of the Franchise Agreement – which only allows the provision of broadband Wi-Fi, voice communications, charging, and electronic advertising display capabilities - the privacy issues raised by the City of New York and Alphabet recording people, recording conversations, and taking photographs is obvious. In effect, the City has allowed the deployment of a **vast technology surveillance network** that includes the use of video, audio, and image monitoring and/or recording on virtually every block in Manhattan, as well as thousands of other locations throughout the other boroughs where the EBKs are/will be located. In addition to this surveillance capability, the EBK video capabilities can capture activities taking place in private homes since the cameras are located almost eleven feet above ground and have 180 degree visibility up and down and side to side. If the cameras have zoom capability, this would allow them to see even greater detail inside residences.

EBKs Raise Serious Constitutional Issues Under the 1st, 4th, 5th, 9th, and 14th Amendments

The vast network of 10,000 EBKs violate individual and group Constitutional rights under the 1st, 4th, 5th, 9th, and 14th Amendments since mobile device data and metadata can be obtained by the City of New York under the provisions of the Franchise Agreement without a warrant or any judicial oversight. This is particularly true in light of the Supreme Court's June 2018 ruling in Carpenter v. United States. In addition, anonymous data that the City can receive under the Franchise Agreement – aggregated or otherwise – can be personally identified by cross-referencing it with other databases using business analytic software applications (also unconstitutional). Equally as important, the audio recording, video recording, and photographic capabilities also violate each of these Constitutional rights. And finally, the required geographic deployment strategy of the EBK units violates the 14th Amendment's "equal protection" clause.

EBK Wi-Fi and Video Capabilities on Virtually Every Block Raise Privacy Issues for Motorists and Bicyclists

The EBKs pose a tracking and surveillance issue for motorists and bicyclists. EBKs could be used to track motorists through license plate recognition performed either through automatic license plate reader technology (ALPR) or through video recording and photographic capabilities used in conjunction with off-line image readers. The units also can track both motorists and bicyclists by capturing a mobile device's unique ID (MAC Address) transmitted by their cell phone or other mobile device. And for motorists with on-board vehicle Wi-Fi, the same is true. Motorists and bicyclists do not need to be using the EBK Wi-Fi service in order to be tracked since their devices always transmit their unique device IDs. Using any of the aforementioned methods, Alphabet and the City can identify and track motorists and bicyclists down to the block, garage, or building - 24/7/365 - anywhere in Manhattan and the other boroughs where EBKs are/will be deployed.

All EBK Wi-Fi Units Incorporate Hardware and Software Capabilities That Are Unauthorized By the Franchise Agreement and Thus Violate the Contract

The Franchise Agreement allows only Wi-Fi, charging, voice communications, and electronic advertising display capabilities to be built into the EBK units, but each one contains hardware and software for the following: video recording, audio sensing, audio recording, photographs, and Web access via direct manipulation of an EBK's video screen. None of these capabilities is allowed by the Franchise Agreement and thus all EBK units are in material breach of the contract.

The City of New York May Have Wanted to Install EBKs in Order to Create a Massive Surveillance Network

The City of New York may have wanted to install the EBK Wi-Fi network, along with audio, video, and photographic capabilities, with the ulterior motive to implement a vast surveillance apparatus throughout the five boroughs. The fact that the City has free, unlimited, on-demand access to all mobile and home device metadata captured by the EBK Wi-Fi network - as well as the inclusion of audio, video, imaging, and recording features into the units – is prima facie evidence that it wants to use the 10,000 LinkNYC EBKs as a massive surveillance network.

The Stop LinkNYC Primer

Free Broadband Wi-Fi Service Provided by Alphabet and the City of New York's Public-Private EBK Monopoly Franchise Harms the Competitive Market for Fee-Based Wireless and Wireline Services

Alphabet (and the City) is able to provide free Wi-Fi services because it uses its monopoly position of using the City's sidewalks to display advertisements that are paid for by private companies. The ability of the monopoly Wi-Fi franchise to offer free broadband communication service is anti-competitive because it undercuts the equilibrium price for fee-based broadband communication services offered by wireless and wireline communications vendors who do not have the same access to the City's sidewalks. One of Alphabet's business objectives, which it has published in its marketing materials, is to use its anti-competitive pricing model to siphon customers away from fee-based wireless and wireline broadband service providers (such as Verizon, AT&T, T-Mobile, Spectrum Cable, etc.). It can also do the same with non-broadband services, such as voice and text.

The City of New York and Alphabet/Sidewalk/Intersection May Have Colluded to Decimate the Existing Wireless and Wireline Markets in Order to Reap Massive Monopoly Profits and Other Benefits for Themselves

The public-private Wi-Fi monopoly is using its privileged position of being the sole entity that has access to the City's sidewalks to provide wireless broadband service in New York City. It offers comparable Internet speeds to those of wireless and wireline carriers and are provided for free, financed primarily by fees generated by electronic advertisements shown on the LinkNYC EBK screens. Since the City and Alphabet can offer its wireless broadband service for free, it may be able to siphon off a material number of customers from existing wireless and wireline broadband vendors. By doing this, they potentially will be able to generate a high level of revenue for their public-private monopoly. In Year 8 of the Franchise Agreement, the City becomes the de facto majority owner of the monopoly since it will begin to reap over 50% of the revenues. The potentially massive financial reward to the City creates a number of conflicts of interest, particularly with respect to seeing the competitive market for broadband service be harmed (or disappear) as well as to the physical and mental well-being and privacy of its residents and visitors.

The LinkNYC EBK Wi-Fi Service Raises Potential Health and Transportation Issues

The Wi-Fi units contain industrial strength access routers that could emit RF radiation that could harm people of all ages who stand next to, work near, or walk by the units. In addition, the City may want to go beyond the Franchise Agreement's legal limitation to provide Wi-Fi service and allow the Department of Transportation to use the units for tracking vehicles, surveillance, traffic enforcement, and transportation-related projects and goals.

The City's Contract with Alphabet Raises the Possibility of Ethics, Administrative, and Legal Violations with Respect to How the Franchise Was Awarded and How the Wi-Fi Units are Deployed Throughout New York City

Alphabet (Sidewalk/Intersection) employs three high level executives who were former officials of the City of New York. They are: Daniel Doctoroff, Chief Executive Officer (CEO), who was a former Deputy Mayor of Economic Development; Joshua Sireman, Chief Development Officer (CDO), who was a former Chief of Staff to the City of New York's Deputy Mayor of Economic Development; and Rohit Aggarwala, Chief Policy Officer (CPO), who was a former Director of the Office of Long-term Planning and Sustainability. Mr. Doctoroff, Mr. Sireman, and Mr. Aggarwala each may have had direct control or indirect organizational influence over New York City departments that were involved in: 1) evaluating the actual need for free public Wi-Fi, and/or 2) granting the franchise to the company of which they are now CEO, CDO, and CPO, respectively. That three C-level positions within the company are held by former City of New York officials - who may have been able to influence the justification for a free public Wi-Fi network as well as influence the award to a company of which they are now high ranking executives - potentially raises ethical and legal issues regarding: 1) the entire process the City initiated in considering deployment of free Wi-Fi service and 2) the process by which Sidewalk/Intersection (at the time, CityBridge) was chosen to be the monopoly franchisee. In addition, there are legal and ethical issues raised by the discriminatory geographic deployment strategy of the LinkNYC Wi-Fi units where Manhattan - which comprises only 7% of the City's land area - is required to receive 52% of the required 7,500 units (or, 3,900) when it has only 17% of the City's population, and an even lower percentage of those who can't afford paying for Internet service. This deployment strategy is not consistent with the City's and Alphabet's claim that the need for a free public Wi-Fi network is to close the digital divide for the "over 25% of New Yorkers who lack high-speed broadband service".

Background on Corporate Structure of Alphabet

For readers to understand the assertions and claims made in this document with respect to the LinkNYC Wi-Fi network operated by Sidewalk/Intersection, it's worthwhile to review a short explanation of the corporate history and structure of Alphabet, as well as what the overall business areas it's involved in and how it makes the vast majority of its money.

The City of New York awarded a monopoly franchise to provide free broadband Wi-Fi service in New York City to a company called CityBridge. The service is provided by Wi-Fi units installed on the city's sidewalks, typically at intersections of streets and avenues. The service is financially supported primarily by private companies buying digital advertisements on the units' massive electronic billboards. There is also a fee-for-service revenue stream, but it is minor compared to the revenue generated by advertising fees.

CityBridge was created by four companies: Titan, Control Group, Comark, and Qualcomm. CityBridge merged with a company called Intersection, which was led by another company called Sidewalk Labs. Sidewalk Labs is a corporate subsidiary of a company called Alphabet. Prior to being called Alphabet, the company was called Google. Google is a well-known Internet company that offers many types of Web services including Google Search, Google Mail (or Gmail), Google Maps, and more. In addition, it has a multi-billion dollar digital advertising platform called AdSense that is used to serve advertisements to its own and 3rd-party websites.

As Google expanded its scope of activities over the years to areas beyond its traditional Web businesses, the company decided to change its name to Alphabet in order to move away from the narrow connotation that the brand name "Google" represented. The new name, Alphabet, would better reflect the many different market segments it was operating in, such as Web services, mobile devices, robotics, transportation, healthcare, and digital eyewear just to name a few.

Alphabet is a public company and trades on the New York Stock Exchange under the symbols GOOG (Class C stock) and GOOGL (Class A stock). Since Sidewalk/Intersection is a company that Alphabet/Google owns, the entity with whom the City of New York entered into the public-private partnership to deploy the LinkNYC Electronic Billboard Kiosks (EBKs) will be referred to henceforth as Alphabet, and as Sidewalk/Intersection and CityBridge where appropriate. At the end of the day, Alphabet, Google, Sidewalk/Intersection, and CityBridge are one and the same company – Alphabet.

Alphabet's Business Model

Alphabet is a well-known and dominant Web company that provides various services to consumers via the Internet for free (it also has some fee-based businesses but they constitute a relatively small percentage of its overall revenue). The company's primary revenue generation model is selling digital advertisements. Alphabet generates this revenue by charging companies to advertise on its various Internet/Web services, including the LinkNYC Electronic Billboard Wi-Fi Kiosks (EBKs). Some of the Web services for which it charges companies to advertise on include Google Search, Google Mail, and Google Maps, as well as other websites. In addition, it also owns an advertising services business called AdSense, which companies use to purchase ads for their web sites.

In 2016, 88% of Alphabet's \$90.3 billion in revenue came from digital advertising fees, and the vast majority of that from its Google business. The company uses various mechanisms and corporate assets to generate and serve digital advertisements to mobile devices and personal computers, including: unique device IDs (MAC Addresses), device metadata, personally identifiable information (PII), Internet Protocol Addresses (IP Addresses), service usage metadata, geographic location data, Cookies, Web Beacons, Pixels, Website behavioral and content tracking, unique advertising identifiers, unique device identifiers, and more.

The Stop LinkNYC Primer

Alphabet's Revenue Model Benefits From Capturing Mobile Device and Computer Metadata, Personally Identifying Information, and Web Content and Wants to Collect this Data From the LinkNYC EBK Wi-Fi Network

Alphabet, through the terms of its Franchise Agreement with the City, will be able to collect what will be hundreds of millions, and perhaps billions and trillions of data points about pedestrians, vehicle drivers, vehicle passengers, and bicyclists each year – for both non-users and users of its Electronic Billboard Wi-Fi Kiosks (EBKs). This is true for people who live in New York City, commute to the city for work, or visit as tourists. To put the high volume of data Alphabet will capture in context, if it is assumed that there are 10 million unique mobile devices (phones, tablets, Wi-Fi-enabled vehicles, etc.), and each passes within the Wi-Fi range of 10 EBKs every 24 hours, that's 100 million data points per day that the Wi-Fi network could capture. Over a year, it would be 36.5 billion data points. If each mobile device gets within the Wi-Fi range of 100 EBKs a day, the number of data points captured by the units each year is 3.6 trillion. The volume and granularity of this data means that Alphabet (and the City) will be able to compile a vast amount of extremely granular information on the location of devices and individuals, the amount of time they spend in any particular location, and the routes they walk or drive...down to the block or building, 24/7/365. Again, the capture of this data applies to both users and non-users of the EBK Wi-Fi services. The Privacy, Tracking, Surveillance, and Constitutional Rights section of this document explains how the EBKs will track both users and non-users of the Wi-Fi service.

Since Alphabet's advertising model benefits from the type and amount of data it captures from mobile devices and computers, it can use this information to charge higher advertising fees and thus generate higher revenue. And since under Section 6.3 of the Franchise Agreement the City of New York will receive a percentage of the company's EBK revenue, it reaps an ever-increasing amount of money in proportion to the increase in EBK advertising revenue. Section 6.3 of the Franchise Agreement provides for a 50% revenue split between the City and Alphabet of both advertising and non-advertising revenue through Year 7. In Year 8, the City's share of advertising revenue rises to 55% while the non-advertising revenue remains at 50%. If the percentage amount in any year does not exceed the minimum franchise fee payment, then the minimum fee must be paid (also specified in 6.3).

Since the City reaps a percentage of whatever revenue is generated by Alphabet's advertising model – partly driven by and dependent upon the collection of device data and personally identifying information – it has a strong financial interest in helping the company collect and use as much of it as possible. And because of the percentage-based payment model, starting in Year 8 the City actually becomes the de facto majority shareholder of the public-private Wi-Fi monopoly since its combined percentage-based franchise payments exceed 50% of Alphabet's gross EBK revenues. So while the EBK business is operated and financed by Alphabet, the City of New York is the de facto majority shareholder due to its majority ownership of the revenue generated by it.

Terminology and Definitions

This document has been distributed to people with varying levels of understanding of the LinkNYC EBK network and its underlying technologies. It uses terminology and acronyms that may be new to them so the following list of definitions has been provided for reference.

802.11 Standard – see definition for IEEE 802.11 Standard.

Alphabet – a company with numerous Web and non-Web businesses and subsidiaries, including Google, Sidewalk/Intersection, CityBridge, and Sidewalk/Focus. It owns the assets of the LinkNYC network. Its primary revenue generation model is through selling digital advertisements that are displayed on various Websites as well as on the LinkNYC electronic displays.

Bluetooth - a wireless standard that allows devices and accessories to connect to each other, and which also allows connection to the Internet.

Broadband Service – communication services for video, graphics, and music only. While technically voice and text communications are included under broadband communications, for the purpose of this document they are not because the Federal government provides free mobile phones to anyone who qualifies under its Universal Access program, so providing voice/text service under the EBK broadband Wi-Fi service is not necessary for those who are economically disadvantaged.

CityBridge – the company to whom the initial franchise was awarded to provide free Wi-Fi service and to display digital advertisements. CityBridge was acquired by Sidewalk/Intersection, which is owned by Alphabet/Google.

Data Center – a building that contains networking devices (such as routers), computer hardware and software (such as database servers), and computer storage devices (such as hard disks).

EBKs – an acronym for Electronic Billboard Kiosks. It is used to refer to the LinkNYC Wi-Fi network. See Electronic Billboard Kiosks for definition.

Electronic Billboard Kiosks – the LinkNYC units that provide free Wi-Fi service and display digital advertisements and government messages. This term more accurately describes the dual nature of the LinkNYC kiosks as it includes the digital advertising component of the units and not just the Wi-Fi services component implied by the word “kiosk”.

Franchise Agreement – the legal contract between the City of New York and Alphabet (which includes Sidewalk/Intersection and CityBridge).

Google – a subsidiary of Alphabet that provides various Web businesses such as Google Search, Google Mail, Google Maps, and others.

Hotspot 2.0 – a technical standard from the Wireless Broadband Alliance that specifies how Wi-Fi-connected devices initiate and hold a connection to Wi-Fi access points, such as the LinkNYC EBKs.

HTTP – see Hyper Text Transfer Protocol.

Hyper Text Transfer Protocol – the underlying communications service for the World Wide Web. It allows Internet-connected devices to send and receive information (e.g. Web pages, video, etc.) through the Internet.

IEEE – Institute of Electrical and Electronic Engineers.

The Stop LinkNYC Primer

IEEE 802.11 Standard – the technical standard that defines how Wi-Fi works.

IPv6 – the next-generation Internet addressing specification. Part of its functionality combines a public router’s IP Address with a computing device’s unique ID, or MAC Address. The combined IP/MAC Address is transmitted across the Internet to a destination server, like a website. The MAC Address portion of the combined address is unique and fixed, meaning that a device or user can be geographically tracked by a website for the life of the device. The user’s access to any website also can be tracked. Also, a Packet Sniffer can be used on the transmission to read the MAC Address and geographically track the device. See definition for Packet Sniffer.

LinkNYC – a network of “Electronic Billboard Kiosks” (EBKs) providing electronic advertisements and government messages as well as free Wi-Fi broadband Internet access, device charging, voice communications, and pay-services. It is owned by Alphabet, which also owns Sidewalk/Intersection, the creator and owner of LinkNYC. This document uses the acronym “EBK” – Electronic Billboard Kiosks - to refer to the LinkNYC network.

LinkNYC EBKs – see definitions for LinkNYC, EBKs, and Electronic Billboard Kiosks.

MAC Address – see definitions for Medium Access Control Address and Unique Device ID.

MAC Address Randomization – the ability of a Wi-Fi capable device to generate multiple Medium Access Control Addresses. MAC Address Randomization provides a higher level of privacy for people because, theoretically, it prevents Web companies from identifying specific devices since there is more than one MAC Address for a device, which means there is no unique ID for it. Since there is no unique ID, a Web company can’t create a database profile on a device that could include information on who owns it (personally identifiable information) or how it is used (the location of the device, websites, accessed, web pages viewed, etc.). There are, however, issues with the effectiveness of MAC Address Randomization (see document for discussion).

Medium Access Control Address (MAC Address) – a unique number that is assigned to all devices connected to the Internet. These devices include mobile phones, computers, tablets, as well as many other devices and products that connect to the Internet; for example, digital music players, televisions, vehicles, and other Internet-capable electronic products and home appliances. The MAC Address is similar to a postal mail address, where each residence has a unique address so that mail can be delivered to it. The same is true for every Internet-connected device: each has a unique address called the MAC Address so messages or content – such as web pages, emails, and streaming video - can be sent to it.

Metadata – data and information associated with a Wi-Fi device or a communications message that is sent through the Internet. Examples of metadata that pertain to this document include, but are not limited to, the following: the MAC Address that is captured by a Wi-Fi access point (a LinkNYC EBK), the geographic location where a MAC Address was captured, the time of day a MAC Address was captured by an EBK, the time of day a MAC Address was lost by an EBK, an IP Address, a unique digital advertising identifier, a Cookie, etc.

Network Function Virtualization – the combination of communications networking and computer software functionality into a single piece of equipment.

New York City – the geographic area that includes Manhattan, Brooklyn, Queens, Bronx, and Staten Island. It also refers to specific geographic areas, such as residential or commercial districts within any of the five boroughs.

NFV – see Network Function Virtualization.

The Stop LinkNYC Primer

Non-User – someone who has Wi-Fi enabled (turned on) in their device but does not log into LinkNYC (EBK) access point(s) or use any of its services. Like a user of EBK services, a non-user has their MAC Address (unique device ID) continuously transmitted to the LinkNYC EBK units (also, see definition for User).

On-board Vehicle Wi-Fi – motor vehicles that have Wi-Fi capability either built into them at the time of manufacture or installed as an after-market part. A vehicle that has its Wi-Fi turned on will continuously broadcast its MAC Address (unique ID) to the EBK Wi-Fi network.

Open Systems Interconnection Model – a global standard that specifies how the Internet operates; that is, how the Internet sends messages/information from one device to another; for example, from a mobile phone’s Web browser to a website, and then back to the mobile phone’s browser. It is comprised of “seven layers”, one of which - Layer 2 – pertains to the Medium Access Control Address (see MAC Address). A layer can be thought of as instructions that are used to create, deliver, and receive messages going from one device to another via the Internet. The “seven layers” create packets and frames that contain information (for example, a Web page or email message), which are sent through the Internet to their destination point (for example, a Website like Google Search or Amazon.com, or a person’s email inbox). The OSI Model is a reference architecture for the Internet’s TCP/IP architecture, which contains only four layers. Three layers of the OSI model are combined into a number of the TCP/IP model’s four layers.

OSI Model – see Open Systems Interconnection Model

Packets – how data and information are assembled and packaged for transmission through the Internet. One can think of this as putting an email message or web page content into digital containers (the packets) and then sending them from one device to another (for example, from between a mobile phone and a Website). Packets are like trains, with digital containers (cars) that hold message information (people) and a header (the engine and train conductor). The header contains the information and instructions on where to deliver the contents of the digital containers (either to a Website or back to the mobile/computing device). See Open Systems Interconnection Model.

Packet Analyzer – see Packet Sniffer

Packet Sniffer – a device that connects to a network communications router that captures Internet traffic, such as email messages and Web pages, that is being transmitted from one device to another (for example, from between a smart phone or computer and a Website). A Packet Sniffer can read the MAC Address of any message sent through the Internet. If Alphabet connects a Packet Sniffer to routers in its datacenters, it would have the ability to read the MAC Address contained within an IPv6 IP Address when a person sends, for example, a search request to the company’s Google Search website.

Packet Sniffing – the method and process of reading the data and information contained in packets. See Packets and Packet Sniffer.

Personally Identifiable Information (PII) – data or information that identifies a specific person, including (but not limited to) first name, last name, street address, social security number, driver’s license number, passport number, birth date, birth city, spouses, friends, romantic partners, and more.

PPP – Public Private Partnership (see definition)

Public Private Partnership – a legal entity between a private company and a public entity. For this document it refers to the Franchise Agreement between the City of New York and Alphabet to provide free Wi-Fi service and to display digital advertisements on the LinkNYC EBKs.

The Stop LinkNYC Primer

Sidewalk/Intersection – a subsidiary of Alphabet that provide free Wi-Fi service and displays digital advertisements through its network of LinkNYC units deployed on the streets of New York City. See Alphabet, LinkNYC, and Electronic Billboard Kiosks.

Sidewalk/Focus – a subsidiary of Alphabet that provides transportation-related solutions and services via digital technology.

TCP/IP Stack – Transmission Control Protocol/Internet Protocol software application that allows messages to be transmitted across the Internet. See OSI Model definition for further explanation.

The City – the government of the City of New York

Unique Device ID – a unique number embedded into every Internet-capable device or product at the time of manufacture. It is also called the Medium Access Control Address, or MAC Address; see definitions for both.

User – someone who logs into a LinkNYC (EBK) access point(s) with a Wi-Fi-enabled device or product by using a username and/or password. Devices include mobile phones, tablets, home computers, televisions, and any other product that has Wi-Fi capability. A user has their device's MAC Address (unique device ID) continuously transmitted to the EBKs. A user is also someone who invokes LinkNYC (EBK) Wi-Fi services without logging in; for example, making voice communication calls or engaging any other services that do not require logging in with a username and/or password (also, see definition for Non-User).

Wi-Fi – Wireless Fidelity; an industry standard that allows mobile devices and home computing devices access to the Internet through the air. It utilizes the 2.4GHz and 5.0GHz frequencies of the radio spectrum.

Negative Quality of Life Issues

The deployment of LinkNYC Electronic Billboard Kiosks (EBKs) throughout New York City negatively affects the quality of life of all New Yorkers: it is tantamount to the Times Square-ification of New York City. The physical size of the units, their electronic advertisements, and the voluminous number of them are a visual assault on the senses and the environment; quite simply, they are visual pollution. Appendix 1 contains a map that shows how the required 7,500 LinkNYC EBK units will be massively deployed throughout New York City (another 2,500 units also may be installed, bringing the total to 10,000 units).

The electronic nature of the advertisements is completely unsuitable for both residential areas, mixed residential and commercial areas, and the vast majority of minor commercial districts. It is completely inappropriate for the City to allow these electronic billboards to be installed anywhere other than, perhaps, in a limited number of **major** commercial districts, such as Times Square and Herald Square, and even then only in small, circumscribed areas. From a visual perspective, the EBK form factor and electronic advertisements absolutely are not compatible with the architecture, physical environment, and aesthetics of New York City (henceforth, New York City and NYC will refer to the residential and minor commercial districts in which the EBKs are being deployed; it does not include major commercial districts).

Alphabet describes the size and shape of the EBKs as "iconic" on its website. Nothing could be further from the truth. The EBKs simply do not qualify for this term. More appropriate descriptions are the following: monoliths, leviathans, monstrosities, intimidating, imposing, ugly, garish, visual pollution, cold, icy, unappealing, unaesthetic, disturbing, and – most importantly - distracting. And the fact is, the designation of something being "iconic" is typically done after "the thing" has been around for a long time and there is vast societal consensus that, indeed, the object in question is "iconic". Neither case applies with the LinkNYC EBK units.

Electronic Billboard Kiosks Are Ugly and Distracting

In order for Alphabet to generate advertising revenue, it needs people to look at the EBK electronic advertisements. As such, its goal with the advertising display screen is to be as intrusive as possible to peoples' field of view.

The Unnatural Colors, Bright Colors and Complex Advertising and Message Designs are Ugly and Distracting

The electronic ads and messages use unnatural colors such as bright pink, bright purple, bright white, bright red, bright yellow, and bright green to name a few. These colors are used as backgrounds for textual messages and in graphic-based ads. They fill up the entire screen and force people to look over at the electronic ads since the colors do not fit in with New York City's natural, muted earth tone colors of surrounding buildings, streets, sidewalks, trees, cars, etc.

The unnatural and bright colors make the EBKs stand out from everything else and:

- a) Force people to turn their eyes and heads towards the electronic ads as they walk, bike, or drive down the street,
- b) Force people to look at the electronic ads from three or four blocks away.
- c) Force people to physically turn their eyes and heads away from the units on almost every block they walk if they don't want to see them.

The Complex Graphic Designs are Distracting and Disturbing

Many EBK electronic ads use very complex creative designs that are distracting and disturbing. These designs inject an environmental dissonance with everything around them and are suitable only for dense commercial districts such as Times Square and Herald Square; they simply do not fit in with New York City's residential and mixed residential/commercial areas.

The Stop LinkNYC Primer

The Large Form Factor and Large Screen are Ugly and Distracting

The EBK form factor is over eleven feet (11') high and three feet (3') wide. The screen size is four feet and nine inches on the diagonal, which translates to a vertical height of about four feet and four inches (4' and 4") and a width of thirty (30) inches. The vertical height of the display screen is about 42% of the total height of the EBK.

This imposing, massive height and width of the EBK form factor, and the display screen size in particular, ensures that people will look over towards the units. That, of course, was a strategic decision on the part of Alphabet (as well as the City). The company wants to force people to see the electronic ads from far away so it can show many of them as they walk, bike, or drive down the street. And by locating the display screen well above the height of the average person, the company can ensure that its ads will be seen all the time; the screen can't be blocked by pedestrians' bodies or by most vehicles parked near or driving by them.

It is neither in Alphabet's nor the City's financial interest to have an EBK form factor and screen size that would allow people to see ads only when they are a few feet from the unit. By having extremely large display screens located above peoples' heads and by being able to rotate multiple electronic ads as they walk down the street, Alphabet can increase its advertising revenue. And, due to the variable revenue sharing agreement between the City and Alphabet (see Section 6.3 of the Franchise Agreement), higher revenue for Alphabet translates into higher revenue for the City. So, the City has an important financial interest in allowing the EBK form factor and display screen to be large. Typically, given a 15 second rotation scheme between electronic ads, an EBK can display three or four during the time it takes an average person to walk a short block (i.e., on avenues running north/south).

As mentioned, one of the more distracting and disturbing aspects of the electronic ads is that one is forced to look at them while walking, biking or driving. It is extremely difficult, if not impossible, **to not look away from** the electronic ads. And one is constantly bombarded with electronic ads in their field of view since they are located on almost every block of New York City. This is true for 3rd Avenue and Broadway and it will be true for the entire city if the EBKs are fully deployed.

Another distracting and disturbing aspect of the electronic displays is that one's eyes are pulled towards them even when the units are located across the street, and even when multiple blocks away. This is particularly true when there are few people on the sidewalks, but also true when there are many people around as well as when cars are parked or moving in streets. In either case, it results in one being forced to look over at the EBKs since the brightness and digital advertisement rotation scheme are designed to pull one's head and eyes in the direction of the units. And the reason this occurs is because of the ad rotation scheme, bright colors, unnatural colors, complex creative designs, and large EBK form factor and screen size.

Importantly, **the ad rotation scheme** is a prime factor in the disturbing and distracting nature of the advertisements. It is the **manner** in which electronic ads are rotated that plays a huge role in the pulling of the eyes and head towards them **because a solid black panel is displayed before each new electronic ad that appears on the screen**. The insertion of this solid black panel after a brightly colored electronic ad or message disrupts a person's field of view and forces their eyes and head to turn towards the EBKs.

The physical size of the EBKs, the electronic billboard display screens, the digital ads, and the ad rotation scheme has made the quality of life in New York City much worse since one can no longer look straight ahead while walking, biking or driving...one is now always forced to look at the EBKs and their electronic ads. The EBKs and their electronic advertisements are constantly pulling one's gaze over to them regardless of whether they are on the same side of the street on which one is walking, biking, or driving, or across the street and blocks away. The EBKs have become a constant negative presence in the city's landscape...a disrupting, distracting, irritating, agitating, and hostile intrusion to New Yorkers' daily lives.

The Number of EBK Electronic Advertisements, and The Timing and Manner of Switching Between Them is Distracting and Disturbing

Alphabet's and the City's strategy to rotate electronic ads multiple times in a short period of time ensures that a person will be distracted to look in the direction of the EBKs. The rotation scheme allows three or more electronic ads to be forced upon a person during their walk down a short block, which on average takes 30 to 45 seconds. For motorists stopped at a light, even more electronic ads can be seen since each red light is more than 60 seconds long. **The high number of electronic ads delivered in this short period of time is both distracting and disturbing.** In addition to the negative effect this has on pedestrians, it also raises the question as to whether people who were involved with the project –either City or Alphabet employees – drive or take taxis in New York City. If they don't, they would not understand the distraction and discomfort that frequent electronic ad switching has on drivers, passengers as well as bicyclists. If they do drive in the city, they clearly did not have the foresight to understand the negative effect the electronic displays and ad switching would have on people.

Switch Time Between Electronic Ads

Compounding the sheer volume of electronic ads displayed is the very fast time for switching between them (switch time). This fast "switch time" was established on purpose by Alphabet in order to create a visual dissonance in a person's field of vision so their eyes and head will be pulled towards the electronic ads whenever a new one appears. The fast switch time is not an accident: Alphabet designed it this way in order to maximize the number of times it can force a person to view its electronic ads.

The Manner in Which Electronic Ads are Switched

Compounding the distracting/disturbing nature of the high number of electronic ads and their switch time, is the **manner** in which they are switched. There are two aspects to this issue: 1) the **switch effect** used to transition from one electronic ad to the next and 2) the **solid black screen** that's displayed before a new ad appears.

Switch Effect

The switch effect used to transition from one ad to the next is a "flash", which creates visual dissonance in the field of view. Alphabet planned and designed the switch effect to be a "flash" effect instead of a "dissolve" effect in order to create greater visual dissonance, which forces the eyes and head to turn towards the electronic ads. If a "slow dissolve" effect from one ad to the next were used, Alphabet would not be able to create the high level of visual dissonance it needs to force people to view each successive electronic ad. **This "flash" switch effect was implemented purposefully and is distracting and disturbing; it is totally unacceptable.**

The Solid Black Screen Between Electronic Ads

The solid black screen displayed in between ads is designed to increase the visual dissonance in the field of view, which forces one to turn their eyes and head towards the ads. By transitioning from a brightly colored ad or graphic to a solid black screen, a high degree of visual dissonance is created that ensures the pulling of the eyes and head towards the EBKs (which, of course, will then display the next ad). Alphabet was very purposeful in displaying a solid black screen in between each ad in order to maximize this visual dissonance so that people will continuously look towards the display screen. **The "solid black screen" displayed between electronic ads is distracting and disturbing; it is totally unacceptable.**

In summary, the number of times electronic ads are displayed in the time it takes to walk down a sidewalk, the switch time between electronic ads, and the manner of how electronic ads are switched are distracting and disturbing. Each alone is enough to force the eyes and head to look at the electronic ads and the three working in concert is even worse. The negative physical and mental health effects of the EBKs cannot be overstated. The massive form factor, the massive electronic billboard display, the complex graphics, unnatural colors, and distracting ad rotation scheme cause negative physical and mental health in people. All of it is unacceptable.

And it is worth repeating that Alphabet and the City plan to deploy 10,000 EBKs throughout NYC. This means that peoples' eyes and heads will be forced to turn towards every unit many times during the day as they walk, bike, or drive through the city.

The City of New York Financially Benefits from Visually Dissonant Electronic Ads, Which is a Conflict of Interest in Serving the Public

The City of New York could reap a huge financial benefit from the disturbing and distracting electronic ad scheme, and thus has a conflict of interest in representing and serving the public. Because the City makes more money with higher numbers of people viewing the electronic ads - since Alphabet can increase the number of customers who purchase them and also charge higher rates - it allowed the company to implement the current advertising scheme to the detriment of the physical and mental well-being of its residents.

In order for advertisers to be willing to pay for advertising on the EBKs, they need to be ensured that the City is maximizing Alphabet's ability get people to look over at the display screens. To meet this objective, the City is allowing Alphabet to extract as much pain from the public as it possibly can by allowing it to create a high degree of visual dissonance with the advertising display and rotation scheme. So, while it's against the public's interest to have a distracting and disturbing advertising scheme, the City's financial stake in the public-private partnership with Alphabet is a huge and powerful incentive for it to disregard the mental and physical well-being of its residents. The City has lost its mission to serve and protect its residents due to the fact that it has transformed itself – through its public-private business partnership with Alphabet - from a public entity into a de facto corporate entity that is motivated by profits.

Distracting Drivers with Ads at Intersections Create a Danger for Pedestrians and Bicyclists

Flashing messages at intersections to motorists in a crowded city like New York is not the brightest thing to do by any measure. Distracting drivers approaching an intersection and forcing them to read traffic messages, digital ads, or public service announcements for even one second may mean injury or death for a pedestrian or bicyclist. The one thing drivers need to do when approaching an intersection in New York City is to **PAY ATTENTION SINCE THERE ARE SO MANY PEOPLE WALKING AND BICYCLING**, and not take their eyes off the road to look at messages and digital ads being displayed on a massive electronic screen. It's clear that money was the driving force behind the deployment of the EBKs since it's plain to see that nothing as obtrusive and distracting as large, flashing electronic ads and messages should be anywhere near intersections (that is, crosswalks).

The Electronic Ad Rotation Scheme Violates the Franchise Agreement

The Franchise Agreement with Alphabet states that the electronic ads must “fade” in no less than one (1) second. This requirement is being violated every day by every EBK which a) flashes - not fades – from one ad to the next, and 2) does so in less than one second.

In addition, Alphabet has implemented a **non-ad** in the form of a solid black screen, which the Franchise Agreement does not allow the company to do. The Franchise Agreement allows Alphabet to display only electronic ads, nothing else. As noted in a previous section, the solid black screen is purposefully displayed in between each electronic ad in order to create visual dissonance in the field of vision in order to force a person to look over at the EBK. **The City has failed New Yorkers by not enforcing this provision of the Franchise Agreement.** The City also has failed New Yorkers by the following:

- 1) Allowing Alphabet to switch between ads in only one second (as specified in the Franchise Agreement). This short time frame is much too fast and creates too much visual dissonance, regardless of whether it's done through a flash or dissolve effect. In either case, the short time frame disrupts the field of view and pulls the eyes and head towards the electronic advertisement whenever a new one appears.
- 2) Not requiring a “slow dissolve effect” of no less than five (5) seconds between electronic ads; that is to say, one ad dissolves into the next ad no quicker than five seconds.
- 3) Allowing a solid colored screen (black, red, green, etc.) to be displayed between ads.

The Stop LinkNYC Primer

Electronic Ads are Not Equivalent to Printed Ads

Proponents of EBK electronic ads might argue that there is no difference between them and printed ads (fixed or scrolling) in bus stop shelters, pay phone booths, and other structures and buildings, but they would be wrong to make such a claim. Printed ads are different because:

- 1) They are not electronic and so by definition are not as obtrusive and distracting (everyone knows this to be true).
- 2) For bus shelter printed ads that scroll, the rotation of the number of ads is not as frequent as it is for EBK electronic ads, so one is not subjected to multiple ads walking down a block.
- 3) The rotation method for printed ads causes less visual dissonance than the “flash switch” effect used by the EBKs.
- 4) For scrolling bus shelter printed ads there is no equivalent of the “black screen” that is displayed in between EBK electronic ads, which means less distraction to people.
- 5) There are fewer bus stops than EBKs, so fewer printed ads are displayed and fewer times one has to see the mechanism rotate.
- 6) Printed ads do not use the same bright and unnatural colors that the EBK electronic ads use.
- 7) Printed ads do not contain the high number of different colors that EBK electronic ads use. The numerous and constantly changing color schemes of EBK electronic ads is a disturbance to the aesthetics of New York City residential areas and to one’s field of vision.
- 8) Printed ads do not contain the high number of different shapes and complex designs that are used in EBK electronic ads. The numerous shapes and constantly changing creative designs of the electronic ads is a disturbance to the aesthetics of New York City and to one’s field of vision.
- 9) Printed ads do not have the video and audio capability the EBK electronic ads can have, which are allowed under the Franchise Agreement.

As a Consequence of the City’s Approval of EBK Advertising Display Screens, it also Approved Electronic Advertising for Bus Shelters

Following on the deployment of the EBK electronic advertising, in 2016 the City began implementing electronic billboard advertising in bus shelters, which contain even larger screens than those in the EBKs. The City did this based on what it did with the EBK electronic ads, again to the detriment of New Yorkers since the bus shelters are largely in residential areas. This too is the Times Square-ification of residential areas and mixed residential/commercial areas. And, to make things worse, the City has allowed partial and full motion video to be played on these massive screens. The reader is reminded that this video is being played in major residential areas such as on 3rd Avenue which stretches into the Upper East Side, East Harlem, and the Bronx...major residential areas. In addition, the City has allowed advertisements to have even more distracting transitions than that associated with the EBK network, including sliding panels that stop and the re-start in the middle of the transition. The City, presumably, has the same variable revenue generating scheme with the bus shelter franchisee and thus likely sought to deploy the same electronic billboard concept. Again, the City is acting as a corporation seeking revenue and profits, and not as a government that is looking out for the interests of its residents.

The City’s obsession with raising money for itself is blinding it to the harm it’s perpetrating on the people who live in New York City. The people who live here now have massive electronic screens in their residential neighborhoods and are subjected to the high impact and highly disturbing electronic ads around the clock. It’s the case now that when eating at a restaurant and seated outside or near the windows, diners cannot have a normal conversation with each other because they are constantly being distracted by the massive electronic ads and flashing rotation scheme. Even if you look straight ahead at the person you’re dining with you see the flashing and brightly colored ads in ones field of view. This is absolutely annoying, distracting, and harassing. This has negatively affected the dining experience and the quality of life in New York City. Also, since the EBKs can record video and take photographs, diners have their privacy invaded since the units can capture and store the likeness of people with whom they associate. And since the units also record audio, then they can record the conversations of diners as well, with or without video. In addition, in the case of bus shelters, people who sit

The Stop LinkNYC Primer

inside them are subjected to the bright display just a few inches away from their eyes, and to the disturbing flashing from one ad to the next as well as to the partial and full motion video being played.

EBKs And Flashing Light Into Residences and Businesses

The brightness of EBK electronic ads and the flashing light they generate when switching from one electronic ad to the next negatively impacts residential living and commercial work spaces.

Residential Living Spaces Subjected to EBK Light and Flashes

EBKs are located in residential areas close to apartments and are approximately 11 feet high. A unit's display screen is 50 inches high and 30 inches across (4.2 feet x 2.5 feet) and is placed at the upper portion of the unit, reaching almost to the top. The display and its brightly lit, flashing ads and colored screens can be seen by people whose apartments are close to the units, typically up to the first three or four floors. It is unacceptable for the City to allow this type of light into a person's residence. The flashing nature of the light (when ads are switched) makes this even more unacceptable. It means that people must live with flashing lights coming into their units, or viewing them when looking out the window. This is exacerbated during the night or when conditions are dark during the day, such as with heavy cloud cover or inclement weather.

The appropriate government entities that received this document should investigate whether the effect of EBK light and ad switching violate any laws related to housing, especially to habitability, as well as to the placement of electronic advertising in close proximity to residences.

Commercial Work Spaces Subjected to EBK Light and Flashes

Similar to the issue of residential living spaces being subjected to EBK screen light and flashing light, commercial work spaces are as well. Since EBKs are deployed on sidewalks directly outside commercial establishments, they subject employees to their bright light, flashing light, and constant stream of electronic ads for the entire time they work. While this is disturbing enough during daylight hours, it is even more disturbing at night when the light from the electronic ads is more intense. And as a consequence of the more intense light at night, ad switching during this time is also more disturbing to employees.

The appropriate government personnel who received this document should investigate whether the effect of EBK light and ad switching violate any occupational safety and health laws.

EBKs as Entertainment Platforms and the Use of Sidewalks as Entertainment Venues

The EBKs are in violation of City zoning laws and ordinances regarding providing or performing entertainment in public areas. Because EBKs provide broadband Internet service and contain interactive video screens, external audio speakers, and internal audio jacks, it means they can function as entertainment platforms on the City's sidewalks. This is incredibly poor public policy and is in violation of zoning laws and ordinances against conducting or providing entertainment on public grounds. The Franchise Agreement does not negate or supersede the process for acquiring permits that allow entertainment to take place on public lands, in this case the City's sidewalks.

The entertainment that the EBKs provide includes playing music, movies, television shows, music videos, sports programs, pornography, and any other entertainment available on the Internet. All of the audio associated with these programs can be broadcast through the large external speaker or accessed through wireline or Bluetooth speakers that also can broadcast audio to the public. In addition, mobile devices can be connected to the audio jack through a wireline connection, enabling people to loiter for hours entertaining themselves. And they can do this and never drain their battery because they can plug their device into the USB charging port. Examples of EBKs being used for entertainment and the public sidewalks being used as the venue are numerous. The following are just a few examples in 2016:

The Stop LinkNYC Primer

- 1) two individuals watching a boxing match for an extended period of time with external audio on and blasting the show to everyone on the street,
- 2) an individual watching music videos with external audio on ,
- 3) an individual sitting in a personal, collapsible chair watching television using internal audio with headphones,
- 4) two individuals sitting on the ground at the base of an EBK with the structure supporting their backs; both enjoying entertainment through ear phones and their cell phones,
- 5) an individual carrying on a phone conversation in a residential area with the external speaker amplifying and blasting out the other party's voice,
- 6) a male masturbating and ejaculating to pornography playing on an EBK's Web-enabled interactive screen,
- 7) a homeless person sitting on a stool in front of an EBK while asleep at 6:30 am, with a blanket over him and ear phones connected to the audio jack; (he had slept on the stool overnight),
- 8) an individual stopped on his bike in front of an EBK interacting with it. The bike blocked the path of pedestrians walking on the sidewalk, allowing only four feet to walk between it and the building nearest to the unit.

It is somewhere between gross negligence and insanity that the City decided that it would be a good idea to allow EBKs to be used as entertainment platforms by allowing the units to incorporate an interactive video monitor for Web (HTTP) access and an audio jack. **More importantly, these capabilities are in violation of the Franchise Agreement, and therefore illegal, since they are not allowed in the main Agreement's section 4.1.1 (Consideration and General Description of Services) or in SRV Attachment sections 3.3, 4.1.3, 4.1.4, 4.1.5, 4.2, 4.2.1, and 4.2.2.**

And, since the internal audio capability uses a jack to output audio to a headphone, it can also be used to output the audio to an external speaker that could be connected to the unit. The combination of an interactive video monitor and audio jack enables anyone to set up a very loud personal speaker and play the audio along with the video, or just the audio itself (music, for example). The City has absolutely no way to prevent such use of an EBK. This clearly allows Alphabet to have its EBKs used as private entertainment platforms that utilize public grounds – the sidewalks – as the venue.

EBKs as Entertainment Platforms Encourage Loitering in Neighborhoods and Clutter Sidewalks

Because the EBKs are entertainment venues, they encourage loitering in residential neighborhoods. New Yorkers are subject to people hanging out on sidewalks and watching and hearing video programs and audio programs. This is simply not something the City should be promoting. It is not only disturbing to see these scenes play out on the streets, but also dangerous since undesirable and criminal elements can hang out on a sidewalk with an ostensible reason to do so (watching TV or listening to music) and then commit a crime when the time is right.

EBKs Block the Flow of Pedestrians Walking on Sidewalks

When EBKs are being used for voice communications, entertainment, or informational purposes, people block the flow of pedestrian traffic on the sidewalk. So, in addition to the EBKs taking up a sizeable amount of real estate on the sidewalk, there is another two to three feet of sidewalk space being taken up by people. This is not the case with traditional wireline public telephone booths because 1) they are not entertainment venues and thus do not have people loitering around them for long periods of time, 2) have a set amount of use-time based on the fee paid to make a call and 3) the units are designed so that a person can enter them and thus not take up limited sidewalk space; that is to say, a person physically enters the phone booth structure/shelter by walking forward into its open area, which results in less sidewalk space being used, which in turn does not impede the flow of pedestrian traffic. This is not the case with the EBKs, where the interface for the telephone is at least four feet in from the sidewalk. There is no shelter to move forward into like there is with the traditional telephone shelters. So, a person who makes a call takes up valuable sidewalk real estate, blocking the path of people who are walking.

The Stop LinkNYC Primer

The Franchise Agreement stipulates that there must be eight feet of free sidewalk space between the EBK and the building closest to it. For some EBKs there is less than this required amount of space when either one person or a group is standing in front of them. There have been observations where there is less than four feet of sidewalk space available for pedestrians when only one person is using an EBK.

Any situation where there is less than eight feet of clear sidewalk when an EBK is being used is a violation of the Franchise Agreement, and therefore illegal. It is not sufficient to allow 8 feet of space only from the unit when it's not in use; there must be 8 feet of space when one or more people are using it. The fact of the matter is this: the unit's hands-on video interface – and audio jack and charging port - should have been on the same side as the electronic display screens, not on the side facing a building. **This was a serious design flaw in the EBK form factor.**

Access to the Internet via a Web Browser in the Touch Screen Violates the Franchise Agreement.

The Franchise Agreement only allows Alphabet to provide wireless broadband service to Wi-Fi enabled devices. In other words, the Franchise Agreement requires HTTP (Web) broadband access via the EBKs through a mobile phone or other Wi-Fi enabled device and not through direct physical contact with the EBK itself (with exception of voice telephone service which by definition is not a broadband service). This means that the access has to be made wirelessly in the same manner as one would access, for example, Wi-Fi service at an airport or coffee shop. **This distinction is very important because it means that the EBKs contain functionality that is not allowed by the main Franchise Agreement's section 4.1.1 (Consideration and General Description of Services) and the Franchise Agreement SRV Attachment sections 3.3, 4.1.3, 4.1.4, 4.1.5, 4.2, 4.2.1, and 4.2.2.**

Section 4.1.5 of the SRV Attachment explicitly states that the Wi-Fi service is to be provided “to Users of the Internet on Wi-Fi enabled devices”. The SRV Attachment says nothing about providing non-voice Internet service through a video screen or audio jack, and manually operated through physical touch and manipulation. So, what the Franchise Agreement specifies is that **communication services, other than voice communications, can be provided ONLY through Wi-Fi-enabled devices.**

It is clear from SRV section 4.1.5 that both Alphabet and the City have violated the Franchise Agreement by integrating video software (Web browser) and hardware (touch screen video display) capabilities directly into the EBK form factor. These capabilities, combined with the broadband HTTP (Web) service the EBKs provide, allow the units to be used as entertainment venues through direct manipulation of the units themselves, and not through a wireless devices. These software and hardware capabilities must be removed from the units; it is not enough to simply disable them. Both Alphabet and the City created facts-on-the-ground by deploying EBK capabilities that do not comply with the Franchise Agreement. That some EBKs are already deployed does not change this fact and is no reason not to demand that these units be replaced with ones that legally comply with the Franchise Agreement.

For the voice requirements contained in the Franchise Agreement (for local and long distance calling, 311, and 911), only a numeric hardkey pad is needed to meet this requirement, which the units contain. There is absolutely no reason for the EBKs to contain any type of touch screen or display that a user would interact with in a manual way. It simply is not needed for voice calls.

It is clear that the City either:

1) forgot to conduct an acceptability review and test of the EBK hardware and software before the beta test commenced to ensure compliance with the Franchise Agreement, or

2) conspired with Alphabet to deploy illegal units in order to achieve objectives (both Alphabet's and the City's) outside those allowed by the Franchise Agreement (and the public hearing process), or

The Stop LinkNYC Primer

3) is incompetent and has no established workflow and/or legal process to ensure that the EBK hardware and software being deployed conforms to the limited and restricted features, capabilities, and specifications explicitly detailed in the Franchise Agreement and its addendums and attachments.

Again, the illegal functionality – as it relates to entertainment and information services - includes the software and hardware that allows users to manually (physically) interact with the EBKs for non-voice communications. It is this functionality that turns the EBKs into entertainment platforms, which not only violates the Franchise Agreement but also zoning regulations and other ordinances. By including a Web-capable, hands-on interactive video screen within the units themselves, it means no wireless activity is taking place between a user and an EBK, as the Franchise Agreement explicitly states must occur. Rather, a person interfaces with a unit non-wirelessly by using those features embedded in the EBK form factor through manual interaction. This is not what the City or Alphabet said (or say) in any of their literature or documentation as the reason for needing wireless (that is, not manually-accessed) broadband service in New York City.

As New Yorkers experienced with the interactive touch screen in 2016, the City and Alphabet violated the Franchise Agreement by adding Web browser capability to the EBKs, which resulted in absolute havoc on the streets, as previously detailed in the examples provided. Clearly, both had ulterior motives with the deployment of the units and premeditatedly violated the terms of the Franchise Agreement by 1) integrating unauthorized capabilities and 2) encouraging people to use them. Neither the City nor Alphabet can be trusted at this point – due to their willful violations of the contract - and so the touch screen must be removed.

No Telephone Handset Renders the EBKs Difficult or Impossible to Use for Voice Communications

Anyone seeking to use an EBK for voice communications is forced to use its external directional speaker if they don't have or use a mobile device. This is a major design flaw in the units since New York City is extremely noisy. Because of the noise from the city streets, voice users are forced to turn up the directional speaker's volume to high levels, thus disturbing everyone around them and allowing strangers to listen to their conversations. It is clear that very little thought went into what is required to make a quality phone call on the streets of New York City, most probably because Alphabet has absolutely zero experience in on-the-street, public voice telecommunications services, and the City failed to do its job in managing the development of the EBK itself. (But perhaps it's otherwise: maybe the City didn't want a telephone handset because it wanted to install a massive audio surveillance network throughout New York City. See Privacy, Tracking, and Surveillance section for further discussion).

The existing, traditional phone booths have both a telephone handset and a shelter, both of which work in concert to reduce ambient noise and provide privacy to the user. The handset's speaker is brought up close to the ear so the other party's voice goes right into it, and the shelter helps in blocking out street noise. An EBK has no such features; it just has an external speaker that has to be played on high volume which disturbs everyone around it. And, someone using the units cannot have any type of privacy since they must speak loudly into the unit, which means everyone can hear them. This is not the case with traditional public phone shelters. This is why there are very few instances where people use the EBKs for voice calls directly from the units themselves – it is a rarity that one sees someone making a voice call from the units. On the other hand, one does regularly see voice calls being made from the traditional phone booths/shelters. Also, the EBK telephone design is a safety hazard, since if someone makes a call to 911 the operator may not be able to hear what the person is saying due to loud background noise from the streets. And, the opposite is true as well: the person calling 911 may not hear the operator.

Management of Electronic Advertisement Graphics and Colors, and Control of Government Messages

There are no provisions in the Franchise Agreement regarding what types of graphics, colors, and images can be shown on EBK screens. The City has left it up to Alphabet and its advertisers to decide what are appropriate images and colors to display in our residential neighborhoods, and in mixed residential/commercial zones. With respect to the latter, the City takes the position in the Franchise Agreement that commercial zoning takes priority over residential zoning. For example, if a 20 story residential apartment building, with 500 people living in it, sits on top of five retail stores with a total of 30 employees working during the hours from 10am to 6pm, it's the commercial zoning that takes priority. The City makes this claim in the Franchise Agreement because it allows Alphabet to deploy its EBKs anywhere there is a commercial establishment, regardless of the number of residents in the same physical zone.

What this means is that the City is allowing its business partner, Alphabet, to do whatever it wants with respect to the visual advertisements displayed on the EBKs. **This simply is not acceptable.** The needs of the residents in mixed residential/commercial zones take priority over the business needs. If the EBKs are to remain (which they should not as this document argues), the City needs to put parameters around the visuals associated with the advertisements, including: types of colors, color brightness, number of colors, size of graphics, complexity of graphics, etc. The electronic billboards and their "wild west" graphics are destroying the aesthetics and livability of residential areas and mixed residential/commercial areas.

And, on a related matter, the City must change the way it views mixed residential/commercial areas. It must put residents first and businesses second when making decisions related to services that utilize the streets or sidewalks. New Yorkers' quality of life must be given the highest weighting in these matters. **A blanket City policy that allows a private company or public-private partnership to deploy infrastructure assets based solely on whether there's a commercial establishment nearby – and which takes priority over the needs and well-being of residents in the same area - is totally unacceptable.**

Government Communication with the Public

The City of New York has decided, through provisions in the Franchise Agreement, it will interact with its residents, commuters, and visitors through the Electronic Billboard Kiosks, although nobody has asked for this type of one-way dialogue. People should not be bombarded with government messages as part of their daily lives while walking, biking, or driving. It's un-American for the City to take it upon itself to message to people on whatever topics bureaucrats think we should hear.

An example of this is the "See Something, Say Something" government message that was frequently displayed in Spring 2016. Does the City really think people want to see that as part of their daily lives? Or to see it constantly displayed during their, say, two mile taxi ride on a Saturday night? Does the City really think people want to hear anything it has to say at 2:00 am as they head home from a night out? The answer, of course, is self-evident. Likewise, do New Yorkers need to be exposed to idiotic factoids such as this one from Spring 2017: "There are 650,000 dogs in New York City", as they fight their way through hordes of people, trash, dog poop, bicyclists running red lights, and homeless people strewn on the sidewalks? Note to City: "Nobody cares. Leave us alone".

With this new technology now being deployed on virtually every block of New York City, the City will be tempted to communicate with people on perhaps any conceivable topic, concern, or issue bureaucrats think is important. The main issue for the public is to what extent the government should be communicating to its citizens about things it has unilaterally decided we must be informed of. Some questions the public and the City need to discuss are:

The Stop LinkNYC Primer

- 1) Who within the City or Alphabet decides on the topics that they think citizens should know about?
- 2) Who within the City or Alphabet creates these messages?
- 3) What recourse do citizens have if they think the City is engaging in political discourse and picking one position over another in its PSAs and non-commercial advertising messages?
- 4) Why should people be subjected to the City promoting any particular topic, such as “history months” dedicated to one political or social activist group or another?
- 5) Are political and socially oriented messages going to be equitably split between liberals and conservatives? If they aren’t, is this both a Constitutional freedom of speech and equal protection issue?
- 6) Why should people be subjected to various pieces of information or “factoids” about NYC, the world, life or whatever it is some City or Alphabet employee thinks important for people to know?
- 7) Why should residents be subjected to a constant stream of information where they live, when they can easily get it on their mobile phones, home computers, televisions, newspapers, and magazines?
- 8) Why does this City think we need to see a forecast of the weather for the next three days when everyone can get access to this at home?
- 9) How often are the citizens subjected to reading the messages, and what are the criteria for how long messages are to be seen?
- 10) Is there an independent board representing a diversity of views across the social and political spectrum that oversees the development of the PSAs and non-commercial advertising? For example: people representing the environment and people representing gun rights.
- 11) Are NYC Community Boards involved in the creation of messages?
- 12) How is it ensured that PSAs and non-commercial messages are being displayed equitably in all areas of the city?
- 13) Are there 14th Amendment “equal protection” issues raised if the City does not display PSAs in an equitable fashion in terms of 1) number, 2) length of time displayed, 3) size, 4) location, etc? How is the display of different PSAs documented and audited? Who does the auditing?

The fundamental issue that’s raised by EBK public service messages is whether the government, or Alphabet, should be telling citizens anything at all. And the situation with PSAs and non-commercial messages on EBKs is different from those displayed on television, where someone can turn the channel and not see them. With the EBKs you cannot turn away since 10,000 units are planned to be installed on virtually every block of the city.

The Minimum Franchise Fee Payment of \$500 Million Over 12 Years is Not a Material Amount of Revenue to Justify Deployment of the EBKs

The Franchise Agreement between Alphabet and the City requires a minimum payment of \$500 million to the City over a 12 year period, or about \$42 million per year on average. There is the potential for higher fees based on a percentage of revenue generated by the EBKs, which is 50% for advertising revenue through Year 7 of the contract and 55% thereafter, as well as 50% of non-advertising revenue for the entire length of the contract. The amount of \$500 million over 12 years, while seemingly high, in reality isn’t and it does not justify the deployment of 10,000 EBKs throughout New York City. To put this amount of money in perspective, a short analysis can be done to illustrate what it would mean in terms of increasing income taxes to raise an average of \$42 million each year for 12 years.

According to the State of New York’s Finance Department, New York City had 3.84 million tax returns filed in 2013, which is a close enough year to serve as a proxy for this analysis. Of this number, 2.4 million were taxable returns; that is to say, returns where people had to pay tax. To simplify the math for this exercise, the 3.84 million tax returns is rounded to 4 million. At 4 million returns filed, the tax that would have to be raised in order to generate an average of \$42 million/year is \$10.50 per return. This translates to 20 cents a week, or 3 cents a day, in additional income tax that would need to be generated for each return filed.

The Stop LinkNYC Primer

Now, in 2013 there were 2.4 million NYC returns that actually owed tax. This means that a \$17.50 annual tax increase would be needed per taxpayer to generate the \$42 million. This translates to only 37 cents/week, or 5 cents/day, per 2013 return that owed NYC tax. **This is certainly an affordable amount for anyone who pays taxes to the City.**

And even at only 1 million taxpayers, the annual tax is just \$42 annually (81 cents/week or 12 cents/day); a higher, yet still affordable amount for this group of taxpayers.

Clearly, \$42 million in average annual revenue to the City does not justify, in any way, the deployment of 10,000 gigantic, ugly, and privacy-destroying EBKs. **This amount isn't even a rounding error in the City's total 2017 budget of 85,000,000,000 (\$85 Billion). It comes to .0005, or 5/10,000. It's not even noise.**

The following table summarizes the tax increase needed for the number of returns filed in 2013, as well as for returns that actually paid taxes in that year:

2013 NYC Taxpayers or Returns	Annual Tax Increase	Weekly Tax Increase	Daily Tax Increase
4 million RETURNS	\$10.50/return	20 Cents/return	3 Cents/return
2.4 million Taxpayers* (Actual)	\$17.50/taxpayer	37 Cents/taxpayer	5 Cents/taxpayer
1 million Taxpayers**	\$42.00/taxpayer	81 Cents/taxpayer	12 Cents/taxpayer
2 million Taxpayers**	\$21.00/taxpayer	40 Cents/taxpayer	6 Cents/taxpayer
3 million Taxpayers**	\$14.00/taxpayer	27 Cents/taxpayer	4 Cents/taxpayer

* This is the actual number of tax returns that owed taxes in 2013.

** These figures are provided to illustrate the low amount of tax needed at given levels of tax returns filed that owe tax.

Alternative Ways the City can Generate \$42 Million in Revenue per Year

1) Increase Parking and Overall Traffic Fines from between 4.6% and 7.6%

To look at generating the \$42 million annually another way each of the 10,000 EBKs will generate, on average, \$4,200 in revenue for the City each year, or \$81/week. To raise this kind of revenue, all the City has to do is increase parking ticket fines by 7.6%, which means a \$65 parking fine (below 96th street in Manhattan) increases to around \$70. If one can pay \$65 for a ticket, one can pay \$70. The same is true for all the other types of parking fines. In 2014, parking tickets generated \$546 million in revenue for the City and fines for **all parking and traffic violations generated \$890 million.** **To generate an additional \$42 million/year, the City could increase just parking ticket fines by 7.6%, or all parking and traffic fines by just 4.6%.**

2) Reduce City Expenditures

Instead of raising additional money to equal \$42 million per year, the City could cut \$42 million from its annual budget. Private companies regularly must reduce their expenditures to adjust to new economic conditions and the City can do the same. Reducing the City's budget by \$42 million is equal to 5/10,000 (.0005) of the total 2017 budget of \$85 billion.

3) Implement a combination of revenue increases and cost reductions

The City could implement a combination of the three ideas proposed here: tax increases, parking fine increases, and budget cuts.

The Stop LinkNYC Primer

Generating the \$42 million in annual revenue and/or cost saving by the three methods described will save New Yorkers from the grotesque visual blight of the EBK form factor size and electronic ads. Also, and more importantly, it will protect our personal privacy and Constitutional rights (see Privacy, Tracking, Surveillance, and Constitutional Rights section for discussion of these topics). Even if the total EBK revenue to the City were to double to \$84 million a year, either through modified minimum payments or increased revenue from its percentage revenue sharing agreement with Alphabet, that amount could be generated or cut in the ways discussed without being a huge additional burden on taxpayers and the City.

At the end of the day, the guaranteed minimum amount of money the City will receive under the Franchise Agreement simply does not justify the Times Square-ification of every block of New York City. It does not justify, at all, installing massive electronic billboards that display unnatural and bright colors, complex graphics designs, large blocks of solid colors, distracting switch methods and timing, and complex visual ads in residential, mixed residential/commercial, and minor business areas – which comprise the vast majority of New York City.

If the City is so concerned about providing broadband service to citizens who want it but can't afford or get access to it, it can do so by providing financial subsidies that can be financed by raising taxes, raising fees, tax deductions, tax credits, enhancing the free federal phones with subsidies to upgrade to broadband devices, and subsidizing wireline broadband monthly service costs. These would obviate the need to install 10,000 distracting, ugly electronic billboard monoliths deployed on virtually every block of the city. The EBK units already deployed have destroyed the beauty of the city and its residential neighborhoods, and have injected an incredibly distracting element to everyday life. They have also harmed the physical and mental well-being of the city's residents, commuters, and visitors. If either the required 7,500 or maximum 10,000 EBK units are deployed, they will destroy the aesthetics of the entire city forever.

Neither Wireless Nor Wireline Broadband Internet Service are Utilities and Not Necessary or Legally Required to be Provided for Free or at Low Cost

It is important here to make a distinction between broadband Internet service and telephone service. Any qualified low-income individual can receive free wireless cell service via the federal government's Universal Service Fund for voice and text communications. So there is no need to provide free telephone service via EBKs to this population since they already have it. What this means then is that the EBK Wi-Fi network is being deployed for non-voice communications – that is, Internet service that allows this population access to the Web (HTTP service) for high bandwidth applications. Since this is the case, it means that the City wants to provide a **non-utility service for free** to a specific economic class of people living in the five boroughs, and in the process of doing so also provide the free service to those who can afford paying for it. **This is not something the City should be involved with at all.** There is a competitive market for wireless and wireline broadband and Internet service, and the City is not allowed to participate in competitive marketplaces either on its own or via a public-private partnership. To assert that the City is justified in providing a consumer service like this would allow the City to become involved in a market for **any** type of competitive consumer service or product. That notion would be preposterous and contrary to the American way of life.

The Federal Communications Commission has not classified broadband service or Internet service as a utility to which all people must have access, and neither has Congress nor the New York State Legislature. The fact is, **Alphabet does not get to tell New Yorkers what is and what isn't a public utility**, and neither does the City of New York. This is a decision for the aforementioned bodies.

If the City wants residents to have the ability to access broadband Internet services, it should do so by generating the funds through higher taxes and fees as well as budget cuts. It should not try to achieve this goal through the Times Square-ification of New York by granting a monopoly to a private company to display huge, garish, and ugly electronic ads on virtually every block of the city.

The Location of the Beta Test Doesn't Support Alphabet's and the City's Primary Reason for Deploying a Free Wireless Network, Which is to "Close the Digital Divide" for the "over 25%" of the Population Who Lack High-Speed Broadband Service

The City and Alphabet imply – by stating that “over 25% of New Yorkers lack high-speed broadband Internet service” - that this entire population wants the service but either can't afford it or doesn't have access to it. There is no documentation on the City's Department of Information Technology's website that provides independent, statistically significant data supporting its “over 25%” claim.

If Alphabet and the City were really concerned about providing broadband service to this population, the beta test would have focused exclusively in the less wealthy areas where this population lives. Instead of deploying the beta test in the wealthy corridors of 3rd Avenue, Midtown Manhattan, and Broadway below 96th street, it would have deployed the EBKs exclusively in areas such as East New York, Brownsville, the South Bronx, Bed Stuy, and many other areas that are economically depressed. It is the people in low income areas who are least able to purchase broadband services either through a wireline service (such as Verizon's FIOS Cable TV) or through a wireless broadband service provider (such as T-Mobile), and thus are the primary targets for the Wi-Fi service.

The Franchise Agreement's SRV Attachment also shows how the City and Alphabet are putting the majority of EBK units in the wealthiest borough, Manhattan, where the fewest of the “disadvantaged 25%” live. In fact, while Manhattan makes up about 17% of the city's population, it will get 52% of the required 7,500 units (3,900), all of which will have advertisements. Additionally, 42% of the 3,600 units slated for the other four boroughs won't have electronic ads, so the residents of Manhattan are disproportionately subjected to them (See Ethics and Corruption Section for full treatment of this issue). The Franchise Agreement's SRV Attachment Section 1.2.3 (viii) shows the rollout of the required 7,500 Wi-Fi units (by Year 8 of the contract) as follows:

	Number of Wi-Fi Units WITH Advertising	Number of Wi-Fi Units WITHOUT Advertising	Percentage of Units
Brooklyn	767	579	18%
Bronx	361	375	10%
Manhattan	3,900	0	52%
Queens	943	296	17%
Staten Island	29	250	4%
Total	6,000	1,500	

This data is a critically important point to understand, since both Alphabet and the City make the claim that the primary reason to have free wireless broadband service is to serve the “over 25% of New Yorkers who lack high-speed broadband service” and, in their words, “to close the digital divide”. By installing a majority of EBKs in all of Manhattan, it is doing exactly the opposite of what it should be doing, which is to install them in the poorest boroughs and areas of the five boroughs. Clearly, citing the “over 25%” is important to Alphabet and the City insofar as winning and awarding the monopoly franchise but not in actually providing the service to this population. It does not take a rocket scientist to know that 52% of the “over 25%” do NOT live in Manhattan, yet this borough will receive this percentage of the required 7,500 Wi-Fi units. Even if the additional 2,500 units are deployed in the other four boroughs, Manhattan would still have 40% of the units. And this would be far above the percentage of people who “lack” high-speed broadband in this borough. Since Manhattan has around 17% of the city's population, it at most should be receiving that percentage of the required EBK units, around 1,700; assuming it has a proportionate number of the “over 25%” to the other boroughs. It is likely, however, that Manhattan has a lower number of the “over 25%” population so it should be receiving even fewer units. Does anyone truly believe that even one person in the “over 25%” population lives between Madison and 5th in Midtown Manhattan? Why are EBKs being deployed there, or in any wealthy area of the city?

The Stop LinkNYC Primer

The obvious reason that Alphabet and the City did not deploy the EBK beta in the poorest sections of the city first – and are rolling out the majority of EBKs in Manhattan - is because they thought the beta test would be a failure in terms of 1) broadband use and 2) advertising effectiveness. That is to say, the EBKs would 1) not attract enough of the “over 25%” of people who lack high-speed broadband to justify the network’s existence and 2) not provide Alphabet’s national and luxury advertisers a high enough return on their ad expenditures (a huge percentage of the units in the less wealthy areas don’t even have advertisements). After all, the vast majority of EBK advertisements are for products and services that the “over 25%” target population probably can’t afford, such as expensive cars, air travel, jewelry, clothes, spirits, electronics, and more. If they can’t afford to purchase broadband wireless or wireline service, they certainly can’t afford to purchase most of the goods and services advertised on the EBKs. If the justification for the EBKs is to serve the 25% who lack broadband, shouldn’t the units be deployed only in those areas where people are most likely unable to afford it? What would be the reason for “closing the digital divide” in areas where the vast majority of people can afford broadband Internet, get technical access to it, and already have it? (see Monopoly and Competition section for further discussion of this very important question).

A Randomized, Statistically Significant Market Research Study Needs to be Done to Determine the City’s and Alphabet’s Claim that “Over 25% of New Yorkers Lack High-speed Internet” and Actually Want It.

As already stated, the City and Alphabet claim that over 25% of New Yorkers lack broadband service; the implication of which is that they want it but can’t afford it or don’t have technical access to it. The only way to prove the City’s and Alphabet’s assertion is to have a market research firm conduct a randomized survey in New York City, as well as to conduct market research into the ability of NYC households and people to get technical access to broadband Internet (it stretches credulity that over 25% of New Yorkers don’t have technical access to broadband Internet either in their homes or via their mobile device data plans). In order to prevent bias from entering the survey’s methodology, topics, and questions, the market research survey cannot be done in conjunction with any input from Alphabet and vendors who do business with the company. In addition, the City must recruit two independent “watchdog” groups opposed to the EBKs to be part of the process in order to prevent the government from injecting its own bias into the methodology used, the execution of the survey, and the tabulation and analysis of the final results. **Importantly, the survey population sample cannot include people living illegally in the country or New York City: lawful residents and citizens of New York are not obligated to provide a high-speed Internet discretionary consumer service to illegal immigrants. See Ethics and Corruption section for more information on how the market research needs to be conducted.**

Privacy, Tracking, Surveillance & Constitutional Rights Issues

The deployment of a public Wi-Fi network through the LinkNYC Electronic Billboard Kiosks on virtually every block of Manhattan - and on many other blocks of New York City - raises some of the most fundamental privacy and Constitutional issues society has faced to date in the era of digital communications. **Moreover, in light of the United States Supreme Court's June 2018 decision in Carpenter v. United States, the provisions in the City's Franchise Agreement with Alphabet regarding its right to obtain – on demand and for free - cell phone data and metadata generated by the EBKs are unconstitutional.**

This section will:

- 1) Explain how Alphabet's EBKs violate privacy in new and unique ways.
- 2) Detail the various methods Alphabet can **derive** personally identifiable information from so-called "anonymous" unique device IDs (MAC Addresses) captured by its EBKs.
- 3) Explain how Alphabet can determine personal and romantic relationships from the unique device IDs (MAC Addresses) captured by its EBKs.
- 4) Explain how Alphabet can personally identify and track pedestrians who **do not log in to its EBKs**; that is, the **non-users** who merely have their Wi-Fi (or Bluetooth) enabled **but do not use any** EBK Wi-Fi services.
- 5) Explain how motorists and bicyclists with Wi-Fi enabled **mobile devices** will be tracked.
- 6) Explain how motorists with on-board Wi-Fi-enabled **vehicles** will be tracked.
- 7) Explain how Alphabet can monetize the information captured by or derived from unique device IDs (MAC Addresses) it captures from pedestrians, motorists, and bicyclists, regardless of whether they are users or non-users of EBK Wi-Fi services.
- 8) Assert that the City has no operational or technical way to prevent Alphabet from engaging in practices prohibited by the company's EBK privacy policy, as well as having no technical, operational, or legal way to audit whether Alphabet violated the terms of the EBK privacy policy (especially as it relates to non-users).
- 9) Explain how the Franchise Agreement allows Alphabet **to use** unique device IDs (MAC Addresses) to personally identify both users and non-users.
- 10) Explain how the City does not have a published policy around Alphabet's storage of and access to data captured by the EBKs.
- 11) Explain how Alphabet can track Wi-Fi enabled devices, and thus people, down to the block or building 24/7/365.
- 12) Explain how EBK video, photographic, and audio recording capabilities violate personal privacy.
- 13) Explain how EBK video and photographic capabilities can be used to track people.

How a Mobile Device - Like a Smart Phone - Gets a Unique ID (MAC Address)

In order to understand the significant and pervasive threats to privacy that are posed by the EBKs, it's important to understand a little technology behind mobile devices and the Wi-Fi technical standard. This section is written so a person with no technical background can understand how it all works. Also, the threats to privacy that the EBKs raise pertain both to mobile and home Wi-Fi devices, but are more significant for mobile devices. Accordingly, much of this section is devoted to mobile devices.

Each mobile device, home computer, and Internet-capable product that can connect to the Internet has a unique device ID that's given to it at the time of manufacture; this includes personal computers, tablets, mobile phones, televisions, and more. The **unique device ID** is contained in software that comes embedded with the device hardware and is referred to as the **Medium Access Control Address, or MAC Address**. An example of what a MAC Address looks like is this: 3A:HG:IY:44:87:26.

The MAC Address is used in what's called Layer 2 of the Open Systems Interconnection (OSI) model. The OSI model is comprised of seven layers, which specify all of the "communications protocols" used by the Internet to transmit data and information – like an email or Web page – from one device to another. The "communications protocols" can be thought of as a set of instructions. An example of one of these protocols is the Hypertext Transport Protocol (HTTP). The HTTP protocol is used for the World Wide Web, which is a part of the overall Internet. It is used by a Web browser to get access to a Web server (a website). It is part of every Uniform Resource Locator (URL), for example: <http://www.nolinknycbks.com>.

The software in which the MAC Address resides is embedded in a mobile device's hardware called a Network Interface Card (NIC) or in a semiconductor chip; this is true for any computing device that is Internet-capable. It is different from a device's operating system software, such as Google's Android and Apple's iOS operating systems used for mobile phones. It is the MAC Address that plays a critical part in delivering data to and sending data from a mobile device (or any Internet connected device).

As stated, the MAC Address is a unique ID for any Internet device. One can think of it as being like the street address of a home to which the postal service needs to deliver mail. In order for the postal service to deliver a letter to a residence it needs the home's unique street address. Well, the same is true for the Internet, it needs a unique device ID to send emails and web pages to. So, you can think of the Internet as the postal service, and the mobile device's unique ID (MAC Address) as a home's street address. When a mobile device is used for email, voice communications, or accessing web pages, the Internet uses the device's unique ID (MAC Address) to send the message, voice conversation, or web page to it.

How a Wireless Access Point, like LinkNYC EBKs, Capture and Store a MAC Address

There are many technical features associated with Wi-Fi service and one of them is that it allows a Wi-Fi access point (also called a hot spot) like a LinkNYC EBK to capture MAC Addresses (unique device IDs) from Wi-Fi-enabled mobile and computer devices, **regardless of whether they are logged into its underlying Internet service**. When a mobile device has its Wi-Fi turned on, it **continuously broadcasts its unique device ID (MAC address)**. So, when it comes into range of a Wi-Fi access point, the unit captures the device's unique ID and stores it. Since the EBK is a Wi-Fi access point, it stores a Wi-Fi-enabled device's unique ID along with the time of day it picked up the signal. The same holds true for any Wi-Fi-enabled device that is within range of an EBK Wi-Fi signal, such as a home computer, smart phone, iPod, or tablet mobile device like an iPad.

EBK Tracking of Mobile Devices of Non-Users and Users

Because of the networking industry's technical standard for Wi-Fi, the EBKs will capture the MAC Address (unique device ID) of any device that has Wi-Fi enabled (turned on), regardless of whether it's logged into the service. This means that both "non-users" and "users" can be tracked by Alphabet when they get within a unit's Wi-Fi range, which is a minimum of 150 feet, and up to 400 feet.

For definitional purposes: a "user" is a person who has logged into an EBK with their mobile device with a username and password, and a "non-user" is a person who has their mobile device's Wi-Fi turned on but has not logged into an EBK. The Franchise Agreement allows Alphabet to provide Bluetooth wireless service as well, which means that if a person has their Wi-Fi turned off but their Bluetooth turned on, they also may be tracked since a mobile device's unique ID is transmitted over the Bluetooth radio frequency just like it is over Wi-Fi.

The EBK Network Will Capture Unique Device IDs (MAC Addresses) 24 Hours a Day, Which Will Allow Alphabet to Locate and Track Devices and People Throughout the City at All Times

The technical standard for Wi-Fi service, IEEE 802.11, requires that a device's unique ID (MAC Address) be continuously broadcast at all times via the radio spectrum when a device has its Wi-Fi turned on. The Wi-Fi radio frequencies used in the EBKs are 2.4Ghz and 5.0GHz. What this means is that when a person's mobile device has its Wi-Fi turned on, it will have its unique device ID (MAC Address) captured by every single EBK it falls within range of, even if they never use any EBK Internet services. In other words, the unique device ID is captured even when a person has not proactively logged into the EBK Wi-Fi service with a username and password. Moreover, and critically, this means that Alphabet will be able to **LOCATE** all Wi-Fi enabled mobile devices down to the block or building, 24/7/365. And equally as critical, since Alphabet will own a network of 10,000 EBKs throughout NYC, it will be able to **TRACK** a device virtually anywhere in NYC down to the block or building, 24/7/365. **Again, this is true even for non-users who simply have their Wi-Fi turned on but do not log into any EBKs at all.**

So, because of how Wi-Fi technology works, a mobile device (like a cell phone) with its Wi-Fi turned on becomes a tracking device. And with the EBK network, it's a tracking device at a very granular level because Alphabet will have a network of 10,000 units throughout the five boroughs. Alphabet will be able to track everyone – pedestrians, bicyclists, drivers, and motor vehicle passengers with Wi-Fi enabled mobile devices - down to the block or building, 24/7/365. Additionally, Alphabet can do the same with motor vehicles (not just motor vehicle passengers who have Wi-Fi enable phones with them) that have on-board Wi-Fi built into them, with which many vehicles are equipped today.

The privacy implications of the ability for Alphabet to track MAC Addresses from devices and vehicles is of major importance and will be addressed comprehensively further in this section.

Tracking and Location Via the Bluetooth Technical Standard

If EBKs support the Bluetooth technical standard (which presumably they do since the Franchise Agreement allows it), they may be able to locate and track devices, people, and motorists the same way they do with Wi-Fi. If the unique device ID or unique vehicle ID (for Bluetooth-enabled vehicles) is transmitted via Bluetooth on a continuous basis – as they are with Wi-Fi – the exact same privacy, location, and tracking issues apply with this technology.

To illustrate Bluetooth's threat to privacy with respect to the EBKs, Apple announced in September 2016 that its iPhone will no longer have an audio jack for use with wired earphones. While its Lightning port can be used for wired earphones, Apple is encouraging users to use Bluetooth earphones to connect wirelessly. This means that iPhone 7 users who use Bluetooth will be unable to prevent being tracked in New York City, since they must always have their Bluetooth connection turned on in order to use their phone for voice communications – that is, making and answering phone calls.

How a MAC Address From an Email Message or Web Browser Request Can Be Captured by a Website

In addition to MAC Addresses being continuously transmitted by Wi-Fi enabled devices, they are also transmitted in email messages, web page requests, search requests, voice calls, and all other communications over the Internet (for example, downloading a document from a Website or streaming video). This is done using the next-generation IP addressing standard called IPv6, which some Internet-capable devices use now, and which all will use in the future (see the Internet Engineering Task Force at www.ietf.org). The Franchise Agreement's SRV Attachment Section 9.2 specifies that the EBK network must contain state-of-the-art technology, which means that if it doesn't already support the IPv6 standard, it most likely will by the first required technology refresh in year 6 of contract.

The way in which the MAC Address is sent across the Internet by an email message or Web page request with IPv6 is that it actually becomes part of the Internet Protocol Address, or IP Address. The IP Address is used to transport the email or Web page request from a person's device to a Web server, and then back to the device. When the message arrives at the Web server, the IP Address is stored in a log file. Since the IPv6 IP Address also contains the unique ID of a person's device (MAC Address), it means that's also stored in the log file.

Here is how the unique IP/MAC Address is constructed with IPv6:

- 1) A Home or EBK Router's Public Internet Address: 2003:ht5:: (this will change with different Internet providers because each one uses a different router for their own network).
- 2) The Mobile Phone's MAC Address: 3A:HG:IY:44:87:26 (this always stays the same no matter which Internet service provider a person uses. A unique MAC Address is burned into each Internet device).
- 3) The Mobile Phone's Converted IPv6 MAC Address: AHG:IYff:fe44:872 (this always stays the same no matter which Internet service provider a person uses).
- 4) #1 + #3 = IPv6 IP Address of: **2003:ht5::AHG:IYff:fe44:872 (combines the public IP Address of an Internet service provider's router with the converted MAC Address of a person's device).**

So, for an IPv6 Internet transmission, a device's original MAC Address is converted from 3A:HG:IY:44:87:26 to **AHG:IYff:fe44:872, and it is this converted number that becomes the device's unique identification number that can be captured by an Internet service provider, a Wi-Fi service provider, or a Website.**

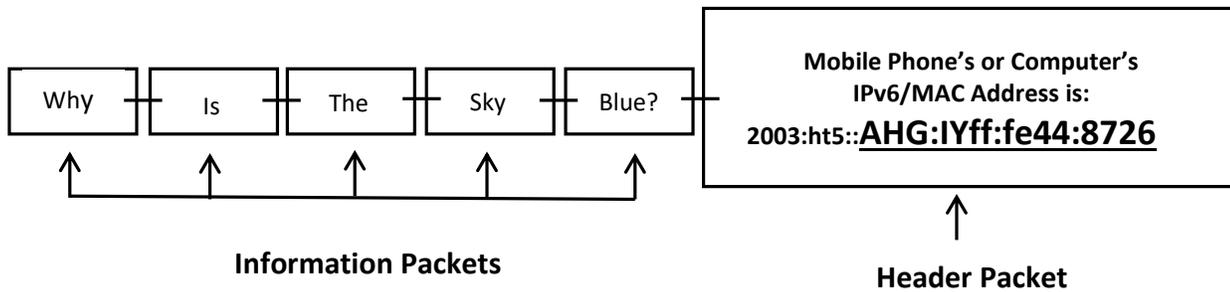
In addition, the original MAC Address is captured by a Wi-Fi service provider's wireless access point, such as Alphabet's EBKs.

How a MAC Address is Sent From a Web Browser to a Website

Information sent through the Internet – for example, Web searches, email messages, social media postings, Web page requests, file downloads – is assembled into a message that contains information packets and a header packet. The header packet contains the instructions on how a message will get from Point A to Point B; that is, from the sender's computer or mobile device to a website.

The instructions are specified in what is called the 7 Layer OSI Model, which is a reference architecture that defines how messages are constructed and then sent through the Internet. The instructions of the 7 Layer OSI Model are embodied in a software application that runs on mobile phones, computers, and any other Internet-connected device. This software is commonly referred to as the TCP/IP Stack. It is the TCP/IP Stack that is responsible for putting information into a format that can be transmitted across the Internet, which includes the information packets and header packet. There are many different pieces of information (instructions and data) contained within the header packet, **including the MAC Address (the unique ID) of a computing device.** Below is a very simple illustration of how a search request - "Why is the sky blue?" - is constructed before being sent to a search website, such as Google Search.

The Stop LinkNYC Primer



The Header Packet includes the converted MAC Address (AHG:IYff:fe44:8726), which is the user's unique device ID. It also has many other instructions that are used to transmit the message from a computing device to the Google Search website.

An Internet or Web company, like Alphabet, has two ways it can read the IPv6 MAC Address when a message or request comes into its website, such as Google Search in this example.

Method 1: Store the IPv6 IP/MAC Address in the Web server Common Log File

Every Web server has a log file that stores IPv6 IP/MAC Addresses from all devices that access it. Once the address is stored, Alphabet can run software programs to read and do analysis on the information associated with it, such as geographic location, time, date, Web pages viewed, search terms, etc. It can run the software so it reads the MAC Address portion of the IPv6 IP/MAC Address; that is, the unique ID of the device accessing Google Search (or any website).

Method 2: Read the Header Packet through Packet Sniffing

A Packet Sniffer (Packet Analyzer) is a hardware device or software application that can look inside the header packet of an Internet message and read what's inside it, including the IP/MAC Address. It could be connected, for example, to one or more of Alphabet's routers in its communications network at its datacenter. The Packet Sniffer "sniffs out" (that is, reads) the MAC Address contained inside the header packet (See Figures 1 and 2 below). Packet Sniffing is a process by which information that's transmitted by a user through the Internet is read by an electronic device or software program. Specifically, Packet Sniffing allows the reading of message content as well as the instructions attached to the message that are used to route it to a website and then back to a user's mobile device.

What this means is that Alphabet can not only capture MAC Addresses from Wi-Fi enabled devices transmitting them to its EBKs, but also when people access its Websites - such as Google Search, Google Maps, and Google Mail – when they use their wireless cellular service or cable-based Internet from home. In addition, if MAC Addresses are sent to Alphabet's AdSense advertising platform by non-Google websites (3rd-party websites) in the course of displaying ads on their Web pages, the company would be able to capture them as well.

So, the multiple methods of MAC Address capture – through EBKs on the streets and through Web logs and Packet Sniffing in its datacenters – allows Alphabet the ability to 1) construct database profiles based on the location and activity of any particular mobile device or computer, and 2) conduct data analytics that can personally identify non-users of the EBK Wi-Fi network. In particular, through data analytics, Alphabet can compile a profile of a person and/or their device by analyzing the device's MAC Address (See Figure 3 below).

Again, a device's original MAC Address always is captured by Wi-Fi wireless access points, like Alphabet's EBKs, when the device has its Wi-Fi turned on (enabled). In the IPv6 world, the MAC Address is converted to a new, unique number when someone actually uses the Internet service to send a message (for example: email, web page request, web search request, social media posting, video or audio streaming, etc.).

The Internet Engineering Task Force (IETF) recognizes the seriousness of the privacy and tracking issues with IPv6 and has a separate working group that has been discussing this matter. See the working group's informational privacy document, Security and Privacy Considerations for IPv6 Address Generation Mechanisms, at https://datatracker.ietf.org/doc/rfc7721/?include_text=1 (ISSN: 2070-1721). Section 3.2 states:

3.2. Location Tracking

Because the IPv6 address structure is divided between a topological portion [**a router's public IP address**] and an interface identifier portion [**a mobile device's MAC Address**], an interface identifier that remains constant when a host [**a mobile device**] connects to different IPv6 links [**different Internet service providers**] provides a way for observers [**owners of a website, like Alphabet with Google Search**] to track the movements [**locations**] of that host [**the mobile device**]. In a passive attack on a mobile host [**the mobile device**], a server [**like Google Search**] that receives connections from the same host [**the mobile device**] over time would be able to determine the host's [**the mobile device's**] movements [**location**] as its prefix changes [**that is to say, as the public router IP address changes**].

So what is being said here is that because the converted MAC Address stays the same in an IPv6 IP Address when a device connects to the Internet using different service providers (e.g. EBK Wi-Fi, home cable Internet, coffee shop Wi-Fi, airport Wi-Fi, etc.), an Internet/Web company like Alphabet can **track the geographic location of the device as well as all of the Websites it accesses**. It can track the device because the company doing the tracking (for example, Alphabet) actually knows the geographic location of service providers' routers throughout the country. For example, it knows that "Communications Company ABC" has an access router located at Broadway and West 34th street in New York City. So when Alphabet's Google Search receives a request from someone's device through that ABC's specific router, it knows the general location the mobile device connected to the Internet. And Google Search knows the specific device itself because its MAC Address is included in the IPv6 IP Address it receives and stores in its log file (or which is packet sniffed from the router in its datacenter that's connected to the Google Search website). So, as a person moves around New York City and uses different Internet services (EBKs, cells service, coffee shop Wi-Fi, etc.), while the router part of the IPv6 IP Address changes, the MAC Address part stays the same. And thus, Alphabet can identify the device (and possibly the person as well) and track them wherever they go.

Figure 1

Figures 1 and 2 illustrate how Alphabet could use a Packet Sniffer (Packet Analyzer) to read MAC Addresses from messages that users send to its various Web services, such as Google Search and Google Mail. Figure 1 illustrates how a message – and its MAC Address - is packaged and transmitted from a user’s computing device, such as a mobile phone or computer. Figure 2 shows how the MAC Address is “sniffed out” (that is, captured or read) by a Packet Sniffer connected to a router in Alphabet’s datacenter, where its Google Search website is located.

Note: The 7 Layer OSI Model is a reference architecture that explains how messages are constructed and transmitted through the Internet. In the real world of the Internet there are only 4 layers, some of which include the other three layers defined by the 7 Layer OSI Model. The 4 layer model is referred to as the “TCP/IP stack” (Transmission Control Protocol/Internet Protocol stack). The TCP/IP stack is software that resides in a computing device’s Network Interface Card (NIC) or in its semiconductor chip.

How IPv6 Packet Sniffing Works – Sending End

Step 1 A Google Search request for “Why is the sky blue?” is sent by a user from a mobile phone or computer via a Web Browser.

Step 2 A set of instructions is added to the search term in a header packet (via each of the 7 layers in the OSI Model), which enables the Web request to be delivered to the Google Search website.

Layer 2 – The mobile phone’s or computer’s MAC Address (Unique Device ID) is added, via Layer 2, to the IPv6 IP Address which is held in the header packet.

Step 3 The search request is sent to Alphabet’s Google Search website through the Internet.

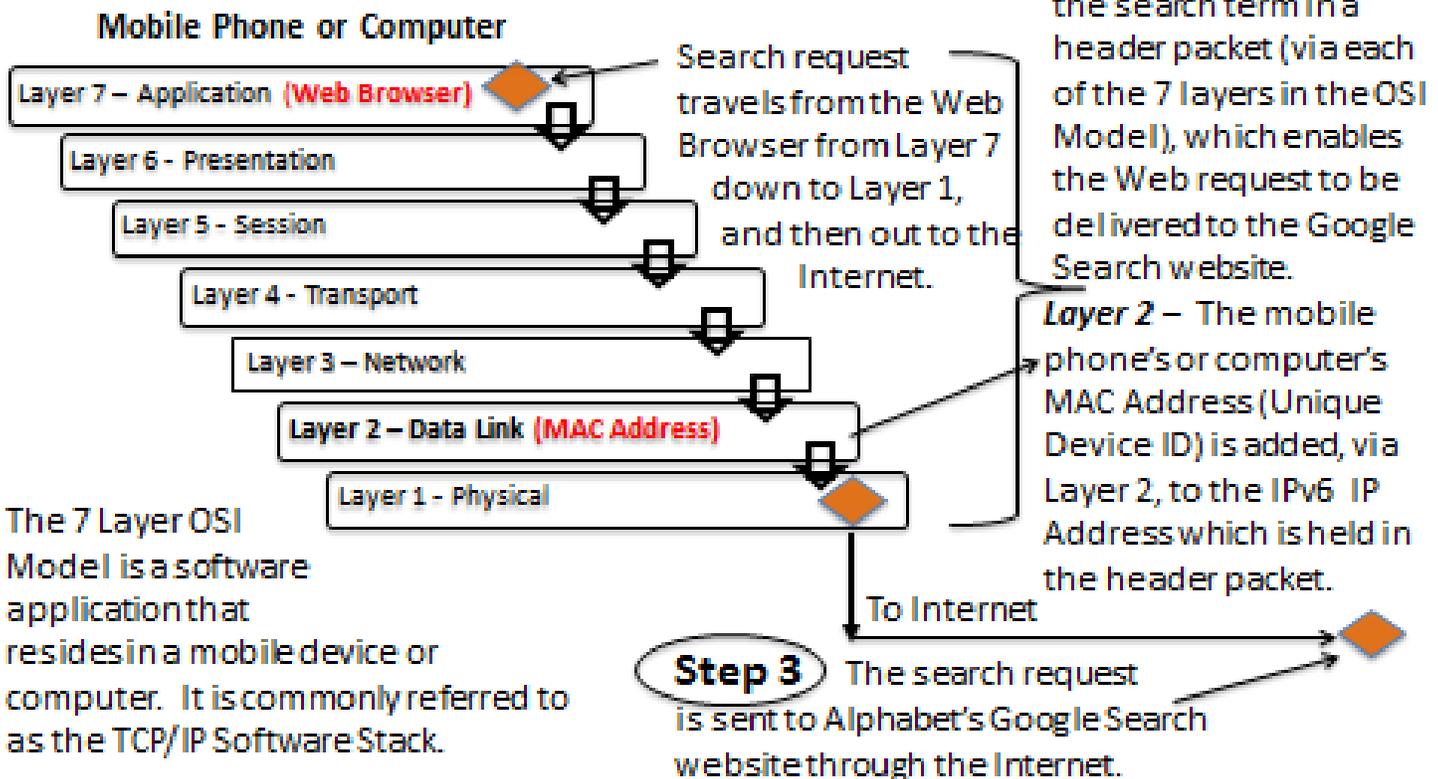
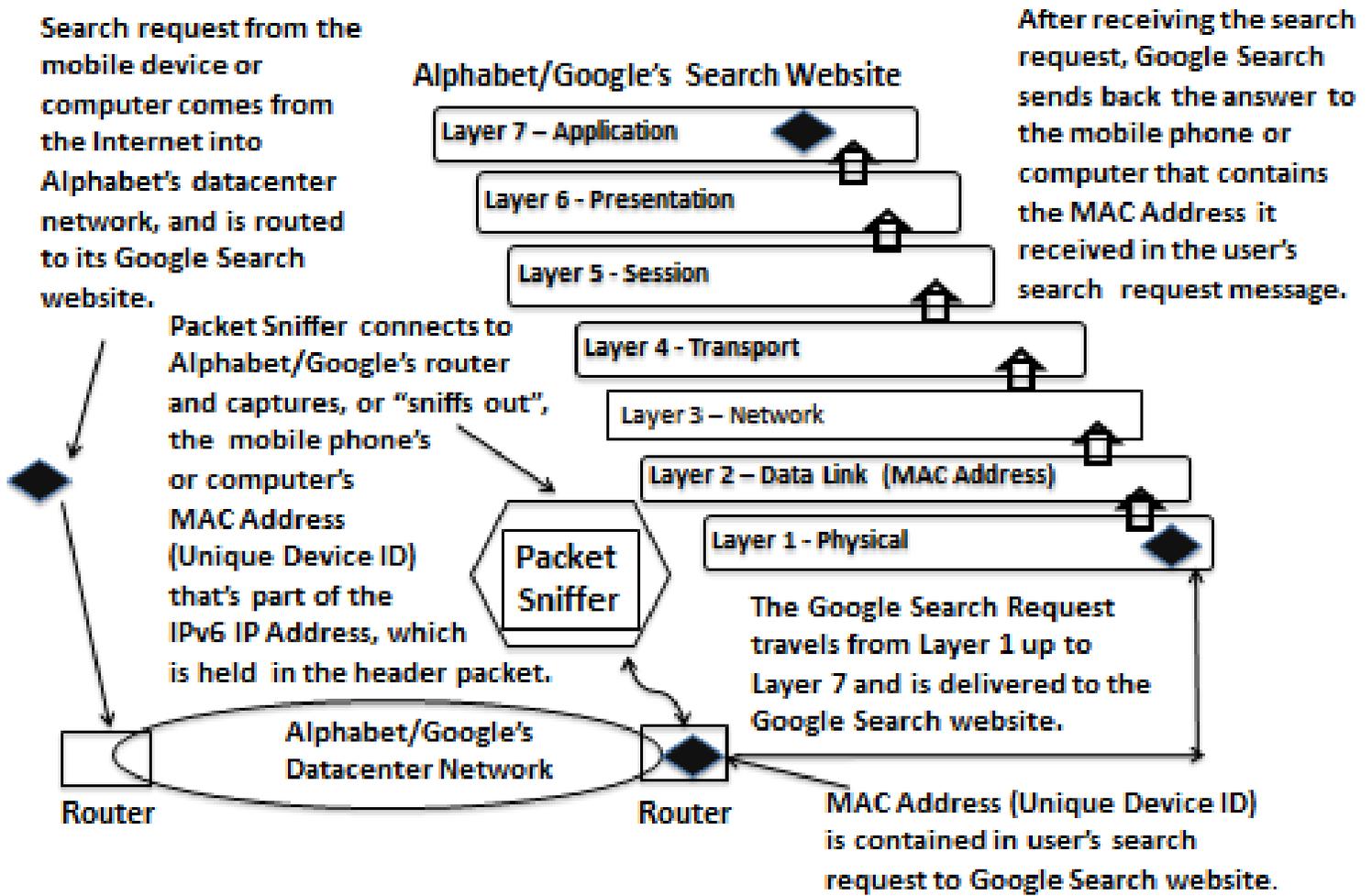


Figure 2

How IPv6 Packet Sniffing Works – Receiving End



How Alphabet Can Match MAC Addresses Captured by its EBKs with MAC Addresses Captured by Using a Packet Sniffer in the Data Center Where its Web Services are Located

Once Alphabet captures MAC Addresses through its EBKs, Web Server log files, and Packet Sniffers, it can consolidate the same unique ID into one profile for a device. Figure 3 below shows three different database profiles – for three different Alphabet web services - for a specific MAC Address. By matching the same ID from these profiles and creating a unified information profile of the device and person who owns it, Alphabet could provide more precise advertising opportunities for its companies who advertise on its various Web services, or who utilize its AdSense advertising platform. It's worth repeating that Alphabet could do this for both users and non-users of its EBKs, since the units capture the MAC Addresses of both.

Alphabet Can Use “Anonymous” Unique Device IDs Captured by its EBKs to Personally Identify People

In the process of combining or cross-reference multiple database profiles it has on a device, **Alphabet also could personal identify someone** (a NYC Council or NYC Community Board member, for example) through their “anonymous” unique device ID by comparing it with unique device IDs it already has stored in other databases it owns **and which** also contain personally identifiable information that is associated to them. Alphabet can do this by using analytic software applications. Because the Franchise Agreement allows Alphabet to conduct analysis on the data that EBKs capture or flows through its Wi-Fi service, it can cross reference the unique device ID data with information in other databases it owns (or purchases from 3rd parties) that contain **both the unique device ID and personally identifiable information that's associated with it.**

For example, take the following situation where a person uses their Wi-Fi enabled cell phone to access the Internet through a home router and also passes by EBKs in Manhattan. Additionally, this person is a registered account holder of Alphabet's email service called Google Mail (Gmail). As a registered user with a Google Mail account, Alphabet may have the individual's personal information contained in a database. This personally identifiable information could include: first name, last name, birth date, age, address, etc. Alphabet also knows the unique device ID (MAC Address) of the cell phone since it has that information from an IPv6 IP Address it captured in the Google Mail log file or through Packet Sniffing.

Now, when the person passes an Alphabet EBK with their device's Wi-Fi enabled, the EBK captures and stores the person's unique device ID (MAC Address), **even though they are not logged into the EBK Wi-Fi service.** Once the EBK has copied and sent the device information to a database server located in its datacenter, the company can then do analysis on it using an analytic software application. It can match the person's "anonymous" unique device ID it captured through the EBK to the same unique device ID that's stored in its Google Mail database **and which** also contains the individual's personally identifiable information contained in their Google Mail account. **When the match is made, Alphabet has just personally identified the person who walked by its EBKs but who never used its Wi-Fi service. Alphabet's act of matching a person's “anonymous” unique device ID (captured by its EBKs) with their Google Mail account information would be done completely unbeknownst to the individual. They have never logged into any EBK service but Alphabet now knows who the individual is, and more importantly, every place they walked, bicycled, or drove in New York City down to the block or building, 24/7/365.**

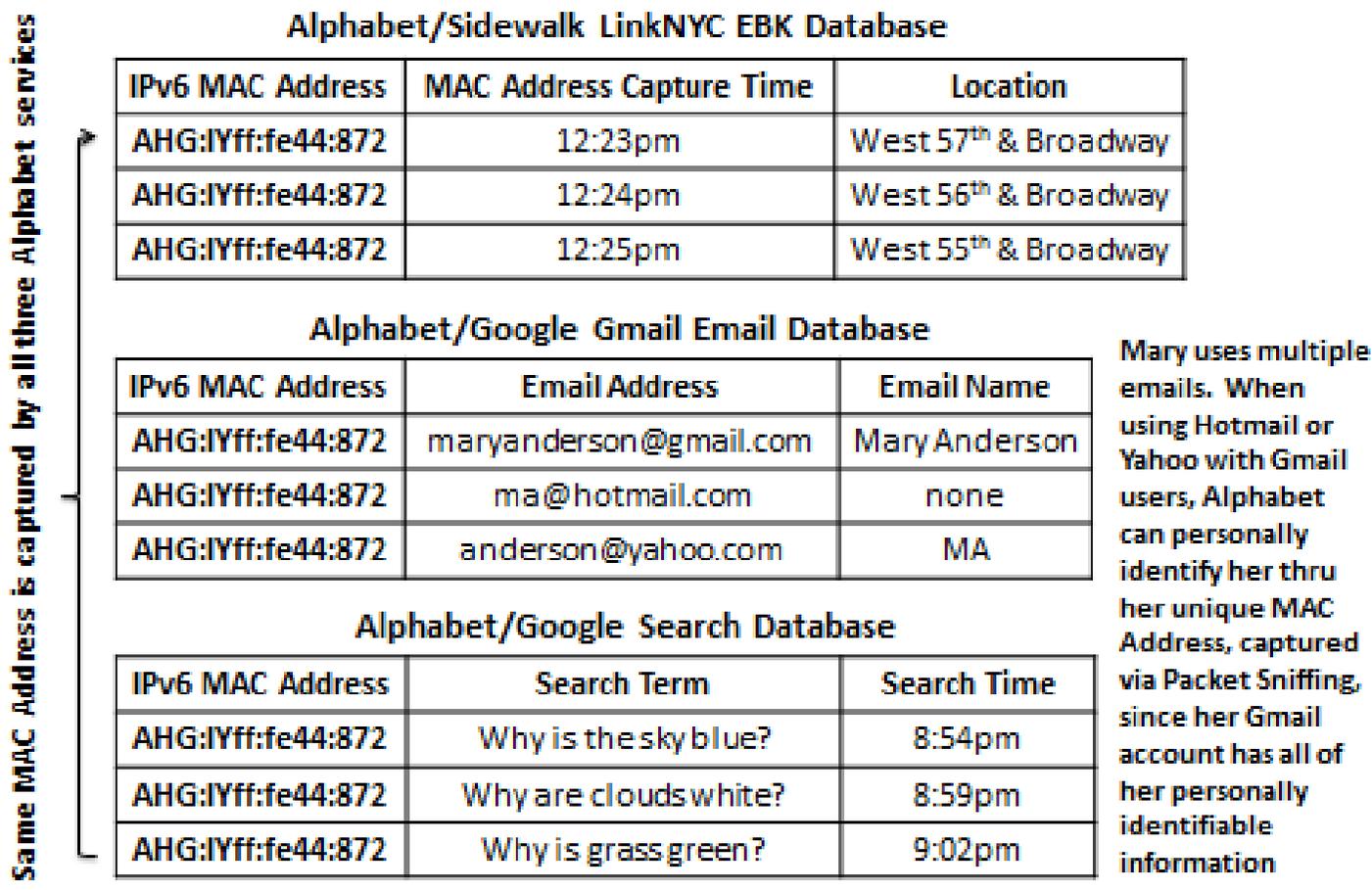
The City of New York, through the Franchise Agreement, allows Alphabet to personally identify people through this manner since it has no restrictions on the company's **internal use** of so-called “anonymous data” or “metadata” once it's captured. The Franchise Agreement only limits and prevents Alphabet from **disclosing** unique device IDs and personally identifiable information, but it doesn't prevent the company from **deriving** personally identifiable information from “anonymous” unique device IDs captured by its EBKs. This raises serious ethical, legal, and Constitutional issues since there is no authorization from non-users (again, the people who don't use EBK services) for Alphabet to: 1) personally identify them, and 2) track their whereabouts throughout New York City wherever its EBKs are located. These same issues also are raised for users of the EBKs (who logged into them) since they may not be aware of the privacy and Constitutional rights implications of their use of the Wi-Fi service.

Figure 3

Figure 3 illustrates how Alphabet could contain multiple database records on a user’s MAC Address. The database records would be associated with each of Alphabet’s Web services and the LinkNYC EBK Wi-Fi network. This example shows three database records for the IPv6 MAC Address **AHG:IYff:fe44:872**, which is stored in Web server or EBK log files, or Packet Sniffed by the following services: 1) Alphabet/Sidewalk LinkNYC EBK Network Database, 2) Alphabet/Google Gmail Database, and 3) Alphabet/Google Search Database.

It would not be too difficult for Alphabet to combine all three database records for MAC Address **AHG:IYff:fe44:872** into a single, larger one. It can also cross-reference the databases to derive personally identifiable information about a user or non-user. **Example 1:** if Mary never uses an EBK but has her Wi-Fi enabled, Alphabet could get her MAC Address from its EBK network and then cross-reference it with the same MAC Address it has for her in its Google Gmail database – obtained from the IPv6 IP Address in the Gmail server’s log file or through Packet Sniffing - since she has an account with this service. Her Gmail account contains personally identifiable information such as her name, address, birth date, age, etc. From this cross-referencing, Alphabet can personally identify and track Mary as she walks through New York City – *even though she never uses EBK services*. **Example 2:** Mary uses three email services – Gmail, Yahoo, and Hotmail. If she uses her Yahoo or Hotmail account to email with Gmail users, Alphabet can personally identify her since the IPv6 MAC Address that’s received by its Gmail service from her Yahoo or Hotmail message is the same one it has for her Gmail account.

MAC Address as the Unique Identifier for Different Alphabet Services



Alphabet Can Continuously Track People Who Use its EBKs Only Once, and Personally Identify Them

If someone creates an account with the EBK Wi-Fi service and uses it only once, Alphabet will be able to track them for the entire time they own their phone. If the individual provides personal information as part of their EBK account set-up, then Alphabet also will be able to personally identify them. This is true because the one-time user – who perhaps just wanted to test drive the EBK service to see how they liked it – always will be transmitting their mobile device's MAC Address to the EBKs if their Wi-Fi is turned on. So even though an individual used the EBK service only once – and provided their personally identifiable information in their initial sign up – Alphabet will track them down to the block, 24/7/365 for as long as they own their phone.

Alphabet Can Personally Identify and Track Mobile Device Owners Who Never Use Its EBK Wi-Fi Service (non-users) but Who Access its Web Businesses via Cell Service, Home Wi-Fi Service, or other Wi-Fi Service

When people use their cell phones to access the Internet through their wireless carrier (for example T-Mobile, Verizon Wireless, etc.), their IPv6 MAC Address is sent to the website they are accessing. This means that Alphabet has a high probability of being able to know anyone's MAC Address, through Packet Sniffing or Web server log files, because the vast majority of people in the country use Google Search, Google Maps, and Google Mail. Moreover, a large number of people have Google accounts that contain personally identifiable information.

All of these Alphabet-owned websites receive a device's IPv6 MAC Address in the process of delivering their services when someone accesses them using their cell phone provider's wireless network. Alphabet can use both the MAC Address it captures at its websites and personally identifiable information it possesses from an individual's Google accounts to identify them when their IPv6 MAC Address is captured by its EBKs...**including non-users. As previously stated, a non-user is someone who has their Wi-Fi turned on in their mobile phone but does not log into or use any EBK services. The mobile phone continuously transmits their MAC Address (unique device ID), so EBKs will always pick it up when they get within signal range.**

So, a non-user of the EBKs can be 1) personally identified and 2) tracked throughout New York City simply by using Google websites accessed through their wireless carrier's cell service. Alphabet can track the person down to the block or building throughout New York City, 24/7/365. The same holds true when a person uses their home Wi-Fi or Wi-Fi from another provider (for example, Starbucks Wi-Fi) to access Google websites.

Alphabet can Personally Identify and Track EBK Users Even When They Use Dummy Account Information or a non-Google Email Address.

In order to use the EBK Wi-Fi service, Alphabet requires a user to create an account using an email address and a password. If someone uses a non-Google email account to access EBK services (e.g. Hotmail or Yahoo email) and also provides dummy information as to who they are, Alphabet still might be able to personally identify the individual and track them. The company could do this because it already may have a database profile on the individual and their device's IPv6 MAC Address. If the individual uses a non-Google email address (e.g. Hotmail or Yahoo) and/or dummy personal information with an EBK account, Alphabet could associate the MAC Address its EBKs capture with the same MAC Address for which it already has the database profile; it could simply add the new non-Google email address and dummy personal information to the existing database record for the database profile it has on the IPv6 MAC Address and its associated device. See Figure 3 above to see a simple illustration of how this looks.

Alphabet Can Store, Copy, and Transmit Unique Device IDs (MAC Addresses) of Non-Users and Users Through Software Programs Running Locally on EBK Hardware or Remotely at Servers in the Company's Data Centers.

EBKs can store unique device IDs (MAC Addresses) in temporary storage, which could be either flash or hard disk storage. Once the EBK has this data in temporary storage, Alphabet can copy and send it to permanent storage in databases located in its remote datacenters, or perhaps even to long term storage hardware embedded in the EBKs themselves. The way it can permanently store this information is by running a software program that copies the unique device ID (MAC Address) - and other metadata (like time and location) - from an EBK's temporary storage area and sending it to a software database application running on a hardware server located at an Alphabet or 3rd-party datacenter (a datacenter is a building or room that contains a large amount of computer and networking hardware and software).

The software that's used to do the copying could be stored and run either in each EBK or from a remote server. The software could instruct the EBKs to send the unique device IDs (MAC Addresses) and other metadata the units have captured at set times during the day or in real time. In addition to sending over the unique device IDs (MAC Addresses), the software also could send the following information:

- 1) The time of day the unique device ID was first recorded by an EBK (that is, the time of day when a mobile device first came within range of an EBK).
- 2) The time of day the unique device ID was lost by an EBK, because the user and their device moved outside the unit's Wi-Fi range or the user turned off the Wi-Fi signal (disabled it).
- 3) The EBK's geographic location.
- 4) The EBK's unit identification number or name.
- 5) Other metadata about the device.
- 6) Information about the EBK Wi-Fi service use.

As already stated, the hardware and software used to execute the copying program could reside in the EBK itself. With a technology called Network Function Virtualization (NFV), computer server functionality and networking functionality are combined into one piece of hardware. This allows running network functionality – such as the Wi-Fi service provided by the EBKs - as software programs. It also means that other types of software applications can be run on the NFV computing hardware, like a simple “copy” software program that would copy and then send the unique device IDs (MAC Addresses) and other metadata to a database server at a remote location. Network Function Virtualization already may be implemented in the EBKs. If it's not today, then it may be in the future since the Franchise Agreement requires Alphabet to re-refresh the hardware and software with state-of-the-art products at various time intervals.

No matter how the copying and sending of the data is performed, **the critical point is that this could be done for both users and non-users of the EBKs.** Again, non-users are those who have their Wi-Fi turned on but do not log into the EBKs (their unique device IDs – MAC Addresses - are captured and stored by the EBKs just like they are with users of EBK Wi-Fi service).

There are No Technical or Operational Ways to Prevent Alphabet from Packet Sniffing, Locating and Tracking People and Vehicles, Personally Identifying, Creating Database Profiles, or Conducting Business Analytics on Users and Non-Users of its Services

Since Alphabet owns the assets of the EBK Wi-Fi network, the City has no technical or operational methods to prevent Alphabet from packet sniffing, locating and tracking people and vehicles, personally identifying non-users, creating profiles on users and non-users, or conducting business analytics on people and their devices. While the city is a majority business partner with Alphabet in the EBK Wi-Fi network (since it reaps a majority of revenue starting in Year 8 of the Franchise Agreement), it doesn't own or manage the network assets itself. This means that Alphabet is free to engage in various technical, operational, and business activities that are against the

The Stop LinkNYC Primer

privacy interests of the public. It does not matter if Alphabet says it won't do any of the things described here because of the restrictions put upon it in the Franchise Agreement and Privacy Policy; **the fact is, the City has no technical or operational way to prevent the company from doing whatever it wants to do.**

There are No Enforceable Legal Methods to Prevent Alphabet from Packet Sniffing, Tracking, Personally Identifying, and Conducting Data Analytics on Users and Non-Users of its Services

While the City may think that the legal terms of the Franchise Agreement and the Privacy Policy are enough to prevent Alphabet from engaging in activities that violate peoples' privacy, the fact is that these are just words on a piece of paper and can't be pro-actively enforced by the City since they don't have any insight into what Alphabet is doing behind the scenes, and never will. For example, while the City could include a provision in the Franchise Agreement to prohibit Alphabet from using a Packet Sniffer in its communications networks, there is absolutely no way it could know whether it's actually using one to read MAC Addresses. The only way it could learn that Alphabet is violating this provision, or some other technical or operational provision, is if a whistle blower within the company came forward, or if something about the unauthorized activities were made public by an Alphabet employee (either accidentally or on purpose). These scenarios, however, are unlikely to happen. Given the nature of Alphabet's business model, the fact it's a publicly traded company, and its practical needs to grow its business in perpetuity, there could be a moderate to high probability that it might engage in activities prohibited by the Franchise Agreement. Alphabet might engage in these unauthorized activities if they could result in an increase in revenue that is higher than any financial or non-financial penalty the City may levy against the company if it found out about the violations. And, because the Franchise Agreement contains no penalties for violating the Privacy Policy or the Agreement itself, there is no legal recourse for the City to penalize Alphabet, which means it has no deterrent to prevent the company from committing any privacy violations.

Federal Constitutional Privacy Issues

Alphabet's ability to capture and store device information, as well as its ability to derive personally identifiable information by utilizing software analytic programs and other databases raises fundamental 1st, 4th, 5th, 9th, and 14th Amendment Constitutional. These civil rights issues are raised because a government entity, the City of New York: 1) granted the monopoly franchise, 2) is involved with Alphabet in the operation of the EBK network, including providing public space for the units, 3) is involved with Alphabet's creation of its EBK privacy policy, 4) can get access to any of the EBK data stored by Alphabet for free and without probable cause or a warrant, and 5) receives financial payments of \$500 million, at minimum, during the length of the contract. As previously discussed, the City will be the de facto majority owner of the public-private partnership starting in Year 8 when it is contractually required to receive over 50% of the revenues.

Section 3.12.5 of Amendment #1 of the Franchise Agreement allows the City to obtain aggregated anonymous data for free. This section does not mention anything about getting the information with a court order or warrant. **In light of the Supreme Court's June 2018 ruling in Carpenter v United States, it means Section 3.12.5 – and any other sections relating to the City's ability to obtain aggregated anonymous data (such as the unique MAC Address) – are unconstitutional. Therefore, the City must remove these sections and be enjoined from receiving any data regarding Wi-Fi enabled devices. This applies to both anonymized data, aggregated anonymized data, or data specific to a particular device, person, or user.** Without the removal of these sections from the Franchise Agreement, it means that the City, without any judicial oversight or warrant, can receive aggregated data for any specific individual's device by obtaining its MAC Address and all the aggregated data associated with it. The City already may possess personally identifiable information on a person associated with their device (obtained through other means), and the City could then personally identify the aggregated data it received from Alphabet. The City could do this by comparing the "anonymous" aggregated EBK data they receive for any particular device (from Alphabet) with personally identifiable data it already has on it, or which it could purchase or receive from another entity like a telephone company, consumer data company, or even Alphabet itself. Or, perhaps more likely, the City could simply ask Alphabet to do the matching of unique device IDs and personally identifiable information using its own company databases, and provide the data back to it in the form

The Stop LinkNYC Primer

of reports. **So, given the current contractual language of the Franchise Agreement, the City of New York, can 1) obtain an owner's specific device information without a warrant, 2) personally identify the owner through data analytics, and 3) locate and track individuals down to the block or building, 24/7/365. The Supreme Court's ruling in Carpenter v United States makes all of this unconstitutional.**

The City's ability to receive computer/mobile device data and metadata raises the following Constitutional issues:

1st Amendment Issues:

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

The government's ability to obtain unique device information (MAC Addresses) from Alphabet means that it can locate and track an individual device throughout the city. By using other information sources that contain someone's personally identifiable information and unique device ID, the government can personally identify an individual's locations and routes of travel throughout the city down to the block or building, 24/7/365. This will have a chilling effect on political speech and on people's right to peaceably assemble at rallies and protests since the 10,000 EBKs that will be deployed in the city will track them at a very granular level. When people realize that every place they go and every move they make with their Wi-Fi enabled devices can be monitored, tracked, and analyzed by the government – whenever it feels like doing so and without court order - at an extremely granular level (down to the block or building) they will be reluctant to exercise certain forms of political speech and assemblage. Specifically, it will chill them from attending political rallies, political forums, educational courses, meetings with government representatives, and more. This is true for both users and non-users of the EBKs.

4th Amendment Issues

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Since, under Section 3.12.5 of Amendment 1 of the Franchise Agreement, the City of New York has the right to obtain unique device information from the EBKs and to derive personally identifiable information about devices using other data sources (such as the account record of the owner of the device from a cell phone provider or personally identifiable information from Alphabet databases), it is violating the entirety of the 4th Amendment. People are not secure in their "papers and effects" and against "unreasonable searches and seizures" since the government can personally identify, locate, and track them down to the block or building, 24/7/365 without probable cause or a warrant. This is true for both users and non-users of EBKs.

5th Amendment Issues

"No person shall....be deprived of life, liberty, or property, without due process of law...."

The 5th Amendment prevents the City of New York from depriving people of their "liberty" (freedom) without due process of law. Since, under Section 3.12.5 of Amendment 1 of the Franchise Agreement the City can locate and track people wherever they go, the Franchise Agreement violates the 5th Amendment because people cannot have liberty if the government can monitor and obtain data on their whereabouts at all times. The 10,000 EBKs will pinpoint people down to the block or building, 24/7/365. Section 3.12.5 is tantamount to the City mandating that a tracking chip be inserted under every person's skin or in their clothing so they can locate and track their movements whenever it wants. There is no liberty when government can locate, track, and permanently store your every move, which is what the City will be doing with the unique device ID data it receives from Alphabet's EBKs. With the deployment of the EBK network, it is the first time in history that a government will be able to electronically track people and/or their personal devices everywhere they go down to the block or building, 24/7/365. This is true for both users and non-users of the EBKs.

The Stop LinkNYC Primer

9th and 14th Amendment Issues

9th: *“The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”*

14th: *Section 1.No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.*

The authors of the Bill of Rights created the 9th Amendment because they did not want the Federal government (and other government entities as well as the People) to think that the ten enumerated rights were the only ones the People possessed. They wanted everyone to know that they retained other rights. An example of how both the 9th and 14th Amendments have been used to acknowledge a right not enumerated in the Bill of Rights or other parts of the Constitution, is the Supreme Court’s abortion decision in *Roe vs. Wade*. It ruled that even though abortion was not mentioned at all in the Constitution, it was still a right “to privacy” that people possessed under the 9th and 14th Amendments. The Supreme Court said, the “right of privacy, whether it be founded in the 14th Amendment’s concept of personal liberty and restrictions upon state action, as we feel it is, or, as the district court determined, in the 9th Amendment’s reservation of rights to the people, is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy”.

Similar to the issue of abortion, people have a right to the privacy of their location and whereabouts under the 9th Amendment and 14th Amendments. No rational American would think that the right to be free from government monitoring and tracking is not a personal right guaranteed by the Constitution. That the City of New York can obtain – without court approval or a warrant - unique device IDs or aggregated anonymized data from every EBK located on virtually every block in NYC – and also derive personally identifiable information related to them - is a violation of both the 9th and 14th Amendments. **This is true for both users and non-users of the EBKs.**

In addition, a 14th Amendment issue is raised regarding the required geographic deployment of EBK units in the five boroughs of New York City. The Franchise Agreement mandates that 52% of the required 7,500 Wi-Fi and Advertising units be deployed in Manhattan, while this borough contains only 17% of its population and 7% of its land area. The high percentage of units being deployed in Manhattan does not support the justification the City gave for approving a free high-speed broadband network. The justification the City (and Alphabet) provided during, and subsequent to, the evaluation process was to serve “the over 25% of New Yorkers who lack high-speed broadband service”. Clearly, putting a majority of EBK units in Manhattan would not meet this objective. The deployment strategy is unable to serve all New York City residents in an equitable fashion. This means that residents of Manhattan and the other boroughs are being treated unequally by the City’s law authorizing the Wi-Fi service, and therefore they are not equally protected. The unequal treatment is as follows: 1) Manhattan residents are forced to accept a much higher number of EBK units than the other four boroughs relative to its population and land area and, 2) Manhattan residents are forced to see more electronic advertisements than the other four boroughs because of #1, and 3) residents of the other four boroughs do not receive the same coverage of free Wi-Fi service as the residents of Manhattan do. In particular, the City’s law - embodied in the Franchise Agreement - violates New York City residents’ “equal protection” rights since it requires Manhattan to bear a heavier burden than the other boroughs to: 1) provide free Wi-Fi to its residents and 2) endure more electronic advertising than the other four boroughs (see Ethics and Corruption section for a more detailed discussion of the Franchise Agreement’s required EBK deployment strategy).

The Stop LinkNYC Primer

The Issues of Unique Device ID (MAC Address) Location and Tracking Associated with Alphabet's EBKs are Not the Same with Providers of Cell Phone Service

Proponents of the EBKs may assert that location identification and tracking by the units is no different from that done by cell phone service providers via their cell towers, which also collect unique device IDs (MAC Addresses), and phone numbers, on a continuous basis. This simply is not true; there are major differences between EBK and cell tower location tracking:

- 1) Alphabet is a monopoly provider of Wi-Fi broadband service in NYC so **only one company** will possess all the unique device IDs and personally identifiable information on all individuals in New York City. With cell phone service, there are multiple competitors so no single company has all this information on every device or person. Only when roaming is turned on will a cell phone's unique device ID be transmitted to a carrier other than the one with whom the person has a service subscription. This is done infrequently though, typically only when the cell phone service provider does not have service or strong signal in a particular geographic area.
- 2) Cell phone technology is different from Wi-Fi technology in that cell towers cannot determine where a person's location is down to the block or building like the EBKs can, without additional operational procedures. The EBKs, as already noted, can locate a person down to the block or building because they will be deployed on virtually every block in Manhattan and many other blocks in the other boroughs. Cell phone antenna towers cover a wide geographic area and cannot, in their normal operation, pinpoint a cell phone to a specific block or building. While they can provide greater granularity on a person's location, it typically takes a court order or an emergency for service providers to invoke the operational procedures and technical requirements to do so.
- 3) Individuals who have cell service have given their consent to their carriers to capture their device information through the act of purchasing the service, whereas they have not done so with Alphabet when they are not logged into any of its EBKs. In addition, their cell phone service providers may already have their personally identifiable information if that is required for people to use their cell service (some pre-paid/pay-as-you carriers do not require personally identifiable information from users of their service). So, a cell phone service customer already knows that their general location will be known to their carrier, and has consented that it can store their device and personal information for the time specified in the company's data retention policy.
- 4) An individual's device and personally identifiable information associated with it is stored for a limited amount of time by cell phone service providers, and then deleted. This is not the case with Alphabet and the City, both of whom will store information captured by EBKs forever. There is nothing in the Franchise Agreement or Alphabet's privacy policy that states data will be deleted after a set and limited period of time, other than that for video recordings – which has nothing to do with device data (of non-users and users) and personally identifiable data generated by the use of EBK Wi-Fi services.
- 5) As noted in the corporate overview section in the first part of this document, Alphabet's business model is to generate advertising revenue using data about devices and people. It uses this data to deliver targeted advertisements and can charge higher fees to its advertisers because of its ability to do this. Essentially, a person's device data and personally identifiable data are core corporate assets for Alphabet, from which it generates most of its revenue. This is not the case with cell phone service providers, who generate cell phone revenue largely through paid subscriptions to their service and not from advertising. Therefore, a cell phone service provider does not have the same incentive as Alphabet to act upon or use location information it obtains from its customers.

The Stop LinkNYC Primer

- 6) Cell phone service providers are private companies, and as such are not able to violate Constitutional rights. By contrast, the EBK Wi-Fi network is partially-owned by the City of New York, and it will become a majority owner of the business starting in Year 8 of the Franchise Agreement when it begins receiving more than 50% of its revenues. The EBK network then, is a government-run communications service, and as such it raises the Constitutional issues mentioned here. Moreover, the Franchise Agreement allows the City to obtain device data and metadata, which is a constitutional violation in light of the Supreme Court's June 2018 ruling in Carpenter v. United States.

Examples of How Alphabet Can Intrude on Privacy with Respect to Personal Relationships and to Individuals

In previous sections of this document, it's been established that EBKs track all Wi-Fi enabled mobile devices through the unique device ID called a MAC Address of both users and non-users. This section will provide examples of how Alphabet and the City could: 1) identify and track individuals and 2) determine relationships between two or more people. The following two scenarios assume: 1) people have their Wi-Fi enabled in their mobile devices, 2) devices are not logged into EBK Wi-Fi service, 3) EBKs are deployed on virtually every block of NYC, and 4) when devices are brought inside buildings, the EBKs lose connections to them (although this may not always be the case in real life since an EBK's Wi-Fi signal range is 150 to 400 feet).

Example #1: How Alphabet can Determine Romantic Relationship Between Two People through its EBKs

Person A is in a new romantic relationship with Person B. Person A begins to visit B's apartment on a regular basis and walks twenty block to B's apartment three days a week. Both A and B exit the apartment on a regular basis to go to a restaurant located ten blocks away, which is the only restaurant on that particular block. After dinner they walk back to B's apartment. "A" spends the night and leaves the next morning at 8:00am.

In this case, the following happens:

- 1) EBKs capture A's new walking pattern to B's apartment because they capture A's unique device ID (MAC Address) as it comes within range of their Wi-Fi signals. This data can be permanently stored in an Alphabet database located in a company-owned or 3rd-party datacenter.
- 2) An EBK outside of B's apartment captures both A's and B's unique device IDs as they exit B's building; the EBK records the time it picks up both of their Wi-Fi signals. They walk to the restaurant ten blocks away; it is the only restaurant on the block.
- 3) As the two walk to the restaurant, they pass 10 EBKs along the way, each of which captures their unique device IDs. This information is permanently stored in an Alphabet database.
- 4) They enter the restaurant and eat dinner for two hours; the EBK outside the restaurant loses their signals after they enter the establishment.
- 5) They leave the restaurant and walk back to B's apartment using the same route; the EBKs capture their unique device IDs along the way.
- 6) When they enter B's building, the EBK outside loses their mobile device signals.
- 7) A sleeps over B's place and leaves the next morning at 8:00am; the EBK outside the building captures A's unique device ID upon leaving the building.
- 8) This same pattern of movement is repeated for six months until A and B end their relationship.
- 9) **NOTE: Neither A nor B logged into any EBKs during their six months together.**

The Stop LinkNYC Primer

In this scenario, a number of personal privacy issues are raised by EBKs capturing A's and B's unique device IDs:

- 1) Alphabet can determine that A and B are in a new relationship because its EBKs capture A's unique device ID for the first time – and subsequent times - when A walks the new route to B's apartment.
- 2) Alphabet knows A's travel route to B's apartment at the block level.
- 3) Alphabet knows the start and stop time of A's walk to B's apartment.
- 4) Alphabet knows how much time A and B have spent together in B's apartment because the EBK located on that block records the time it first picked up A's unique device ID and the time it lost the connection when A went inside the building.
- 5) Alphabet knows the exact time A and B left the apartment because the EBK outside of B's building picks up both of their devices as they exit (If the EBK's Wi-Fi perimeter range is wide enough, it could continue to receive A's device's Wi-Fi signal while inside B's building. In this case, the EBK would record how long A's device was stationary because when A and B leave the apartment and walk to the restaurant the EBK will know at what time it lost A's signal).
- 6) Alphabet knows the route – by block - the two walked to the restaurant.
- 7) Alphabet knows how long it took them to walk to the restaurant by looking at the time difference of A's and B's unique device IDs being recorded by the EBK located on the block of B's building and the EBK located on the block of the restaurant.
- 8) Alphabet knows how long they ate dinner since the EBK on that block captured the time when their devices re-connected with it when they exited the restaurant (if the EBK can still receive their Wi-Fi signals while in the restaurant, it will know when they leave because it will lose the signal when the two depart the restaurant and walk out of its Wi-Fi range).
- 9) Alphabet knows the route they walked backed to B's apartment down to the block.
- 10) Alphabet knows that A stayed over B's apartment since A's and B's Wi-Fi signals were lost at the same time by the EBK outside B's apartment when they entered the building and then A's was picked up again when leaving B's building at 8:00am the following morning.
- 11) Alphabet knows that after six months of dating, A and B decided to end their relationship because the EBK outside of B's building no longer captures A's unique device ID (while still capturing B's on a daily basis), and no other EBKs capture A's and B's unique device IDs at the same time either. Also, Alphabet can see that A is no longer walking to B's apartment because the EBKs located between their buildings no longer capture A's unique device ID as they did when "A" walked the route when they were seeing each other.

Alphabet can know all of this detailed, block-by-block and timing information on the two without either of them ever having logged into a single EBK. The company can generate this knowledge and insight about the two simply from the unique device ID (MAC Address) the EBK units captured, because their mobile phones have their Wi-Fi turned on and their MAC Addresses are continuously being broadcast to the units.

Moreover, both A and B have absolutely no idea that Alphabet is in possession of this extremely personal, granular information that reveals they have a new romantic relationship, details their walking patterns, the restaurant they visit, and that A stays over B's apartment. And Alphabet can reasonably determine that A and B are sexually active since A stays overnight.

If Alphabet already has a database profile of either person with their personally identifiable information (name, address, etc.) from applications the two use such as Google Mail, then it could identify them by running an automated "compare" analytic software program between the EBK database and the Google Mail database, which contains their unique device IDs (obtained from their IPv6 IP Addresses) and personally identifiable information from their Gmail accounts. This software analytic program would use the unique device ID contained in the EBK database and compare it to the unique device IDs in the Google Mail database. When the match is

The Stop LinkNYC Primer

made, Alphabet would be able to personally identify both individuals whose "anonymous" unique device IDs were captured by the EBKs.

Again, all of this information can be captured and derived without A and B logging into any EBKs. Neither one would have any idea that Alphabet is doing this type of analysis. Alphabet could include all the information they derived about the two into permanent database profiles it may already have on them (See Figure 3 above).

Example #2: Determining Where Non-Users and Users Live

Alphabet can determine the approximate or specific building where a device resides or a person lives. The following example illustrates how it can do this:

EBKs are located at the corners of West 75th and West 77th on the west side of Broadway. A woman lives at Broadway between West 75th and West 76th. She does not use EBKs at all - that is, she doesn't log into them but has her Wi-Fi enabled for use in coffee shops she visits. As she walks home from work north on Broadway, the EBK on West 75th picks up her mobile device's unique ID. She then goes into the building where she lives on that block and stays there all night until the morning when she leaves for work. The EBK on West 77th does not pick up her MAC Address.

Since her device's Wi-Fi signal did not get picked up by the West 77th EBK, Alphabet can reasonably conclude that she lives at a building between West 75th and West 76th. To further confirm this, Alphabet can run a simple analytic software program that looks at the time that the EBK on West 75th captured her device ID. If the signal goes dead at 6:30pm when she comes home from work and enters her building, and then is picked up again at 7:30am when she leaves for work in the morning, Alphabet can reasonably conclude the individual lives on Broadway between West 75th and West 76th. If the EBK Wi-Fi signal can reach through the building (which it most likely can), Alphabet still can know she lives in the building because the time stamps associated with her mobile device's transmission to the EBK will show it was stationary (it did not get picked up by another EBK) from 6:30pm to 7:30am.

So, through its network of EBKs capturing this woman's unique device ID (MAC Address) Alphabet: 1) determined that she lives in New York City, and 2) tracked her down to her place of residence on Broadway between West 75th and West 76th. If there is only one residential building on that block, then Alphabet can track her down to her specific street address. **Again, the woman is a non-user of the EBKs**; she has never logged into any of them with her mobile device to use the wireless broadband services. The capturing of her cell phone's metadata (MAC Address and time stamps) and the data analysis have been done without her consent. And the data output and database profile Alphabet has created on the woman is completely unknown to her.

These examples just scratch the surface of how Alphabet can learn about peoples' relationships or locations. Alphabet can do this type of data capture and analysis for either devices or individuals, and it can derive specific information on many different aspects of peoples' lives such as visits to medical doctors, mental health professionals, hospitals, bars, strip clubs, nightclubs, residences, elementary schools, etc. Ultimately, all this information could be used by Alphabet to generate higher digital advertising revenue for itself. All of this information could be obtained or derived by Alphabet for both users and non-users of its EBK services; all the company needs is the MAC Address from computing devices to generate and derive the data. **And again, all of this is unbeknownst to the people who are the subjects of the data capture and analysis. It is important to understand that the Franchise Agreement allows Alphabet to conduct this type of analysis, and to use the data output to generate revenue for itself (and for the City of New York).**

Why Alphabet Would Want to Capture Unique Device IDs from People Who Have Wi-Fi Turned On in Their Mobile Devices But Don't Use its EBK Wi-Fi Service

The reason Alphabet would want to capture device data from everyone, such as the romantic couple and the woman in the examples above, is because it can use that information to: 1) deliver digital ads and 2) provide better targeting for its advertisers. For example, in the case of the new romantic couple, Alphabet may display a digital ad for a neighborhood florist or grocery store to their cell phones when they use them to surf the Web.

Monetization Example

Here's an example of how Alphabet could monetize the MAC Address information it picks up from non-users (and users) of its EBKs, who also use its Google Search service which logs the MAC Address from the IPv6 IP Address.

Jane owns an Android-based smart phone (the Android operating system is owned by Alphabet) and spends three hours shopping on 5th Avenue between 50th and 57th Streets. She has the phone's Wi-Fi turned on but does not use any EBK Wi-Fi services at all. EBKs that are located on each block between 50th and 57th capture her device's unique ID throughout the time she shops. Jane leaves the area and goes home to where she lives in Battery Park. At night, she decides to surf the Web via the T-Mobile cell service she subscribes to and visits various sites. Some of these sites are owned by Alphabet (such as Google Search) and others are owned by other companies who use Alphabet's AdSense advertising platform to serve digital ads that appear on their web pages.

Since Alphabet knows Jane's unique device ID (MAC Address) from capturing it from its EBKs on 5th Avenue for three hours, it also knows that Jane is probably shopping at relatively high-end clothing and personal item stores located on the stretch between 50th and 57th streets. Now when Jane uses Alphabet's Google Search website later that night, the Google Search service knows Jane's unique device ID (its IPv6 MAC Address) through either Packet Sniffing or the Google Search log file. By Alphabet already knowing that Jane shopped on 5th Avenue, it might be able to deliver advertisements to her cell phone for companies who have locations on the stretch between 50th and 57th streets.

This is a form of targeted advertising for which a clothing store (in this example) would be willing to pay a higher advertising fee to Alphabet because it knows it is targeting someone who shops near its store and already may have visited it. So, **without Jane ever having logged into Alphabet's EBK Wi-Fi service on 5th Avenue**, the company could make money from advertisers by merely knowing - via Jane's unique device ID (MAC Address) captured by its 5th Avenue EBKs - she was in the area for three hours. When she's at home in the evening and uses the Alphabet/Google Search website to search for "summer dresses", Alphabet/Google sends back advertisements for five of the clothing retailers located on 5th Avenue between 50th and 57th streets. The company can charge its advertisers more money for this type of targeted advertising than they could if they did not have the location information about Jane that its EBKs captured. So, there are a number of points here:

- 1) Alphabet can capture Jane's unique device ID even though she has not logged into any of the EBKs.
- 2) Alphabet might be able to leverage and make money from her unique device ID data captured by its EBKs with Web services it owns, like Google Search, Google Mail, and Google Maps.
- 3) Alphabet might be able to leverage and make money from her unique device ID captured by its EBKs from 3rd-party websites that subscribe to its AdSense advertising service.
- 4) Alphabet might be able to deliver targeted digital ads to Jane's phone when she uses the Google or 3rd-party website services when she surfs the Web using her T-Mobile cell service (not by using the company's own EBK Wi-Fi network).

The Stop LinkNYC Primer

- 5) Alphabet might be able to charge its advertisers higher fees because it can deliver targeted ads to Jane (because it knows Jane was shopping on 5th Avenue where its advertisers have retail locations between 50th and 57th streets).
- 6) Jane, who is seeing ads on her Google Search page from retailers on 5th avenue where she shopped earlier in the day - **and who never logged into any EBK Wi-Fi service** - has no idea that this type of data processing and sharing of her device information is being done while she is surfing the Web later at night via her T-mobile cell service.

A similar situation exists with 3rd-party websites that Jane visits (that is, websites not owned by Alphabet). Because Alphabet has its own advertising delivery platform called AdSense that these other 3rd-party websites can use, the company might be able to send targeted ads to (Jane's mobile device) through them for retailers on 5th Avenue. It could possibly do this because Alphabet might be able to receive her unique device ID (IPv6 MAC Address) from the 3rd-party websites she visits. If the 3rd-party website sends Jane's IPv6 IP Address over to Alphabet's AdSense advertising service, then it could possibly use it to deliver targeted advertisements based on already knowing she shopped on 5th Avenue. This focused targeting would allow Alphabet to charge companies higher advertising fees via its AdSense business.

Privacy, Tracking, and Surveillance With Respect to EBKs and Motor Vehicles

As with the privacy, tracking, and surveillance issues that EBKs raise with people walking or biking in NYC with Wi-Fi-enabled devices, they pose similar and additional issues with people driving in the city.

Tracking Motorists Through Mobile Devices and On-Board Vehicle Wi-Fi

Alphabet and the City can identify motorists and passengers if they have Wi-Fi enabled in their mobile devices, or Wi-Fi is built into a car as an on-board feature by a manufacturer, or Wi-Fi is added to a vehicle as an after-market upgrade. They can do this because every time a car passes EBKs, the units will capture the unique device ID (MAC Address) from occupants' mobile devices or from the on-board vehicle Wi-Fi.

Alphabet will know that a person is driving or traveling in a car because it can do analytics on the timing of a person's Wi-Fi signal being picked up by successive EBKs. For example: an individual drives up 3rd Avenue at 25 mph for 60 blocks. Each EBK will time stamp the Wi-Fi signal received from the motorist's mobile device or on-board vehicle Wi-Fi. Alphabet can run an analytic software program that looks at the time a device and/or vehicle's on-board Wi-Fi was picked up by each EBK on 3rd Ave. Based on the fact successive EBKs picked up the Wi-Fi signal very shortly after the previous one, Alphabet can determine that the person was driving or traveling in a car.

So a company with whom the motorist has no business or service relationship knows the following:

- 1) that the person drove into the city on a particular day,
- 2) the route they drove through the city,
- 3) the speed of the car (by running an analytic software routine for all the EBKs passed),
- 4) where they parked,
- 5) what time they arrived and left the City.

Again, all of this information can be derived from motorists' and passengers' Wi-Fi-enabled mobile phones/devices and on-board vehicle Wi-Fi. People would be completely unaware that a company (and the City) with whom they have never consented to interact has all of this information on their whereabouts and driving habits.

The Stop LinkNYC Primer

License Plate Number Recognition and Tracking

Since Alphabet's EBKs include video recording capability, it may be able to read vehicle license plates. This of course would be done without the knowledge or consent of those who own vehicles. This is even more troubling if Alphabet could install Automatic License Plate Recognition (ALPR) capability into its EBKs (perhaps they have done so already). ALPR would allow Alphabet and the City to conduct massive license plate reading throughout the five boroughs since they plan to install 10,000 EBKs. By running the captured license plates through a license plate database or an ALPR system, both Alphabet and the City can identify individual drivers and their locations, as well as track them throughout the city down to the block or building, 24/7/365.

The Capture of Unique Device IDs (MAC Addresses) and Other Unique Device Information is Tantamount to Stalking People, Especially for Non-Users

The ability of the EBKs to capture unique device IDs down to the block or building on virtually every street of New York City is a form of stalking; it's passive stalking. If Alphabet employees prowled the streets of New York City equipped with devices to capture mobile device MAC Addresses from people with whom they have no commercial relationship, the company would be charged with stalking crimes. The same would be true if the Alphabet employees just stood at every location where EBKs will be installed and captured MAC Addresses. Nobody would allow either Alphabet or City employees to do this – everyone would consider this a form of stalking. But this is exactly what the EBKs are doing, the only difference being they are inanimate objects doing it. That Alphabet and the City employ the use of hardware and software to capture MAC Addresses – especially from people who do not even use the EBKs - instead of humans holding devices makes no difference....the end result is the same in that they will stalk everyone down to the block or building, 24/7/365.

The public would not accept either Alphabet or City employees actively roaming the streets or standing on virtually every block of New York City capturing peoples' unique device IDs (MAC Addresses) with handheld devices 24/7/365, which means the public does not accept the EBKs passively doing the same exact thing.

Privacy Section 4.4.4 of the Franchise Agreement Allows Alphabet to Use "Anonymous" Unique Device IDs to Personally Identify Non-Users and Users

While the Franchise Agreement's Privacy Section, 4.4.4, prevents Alphabet from disclosing personally identifiable information to third parties without legal authorization, it does not prevent the company from using it internally for operational or "monetization" purposes. Also, it does not prevent the disclosure to third parties of non-personally identifiable information such as MAC Addresses, to which they could subsequently assign personally identifiable information from other information sources.

More importantly, Section 4.4.4 does not prevent Alphabet from using anonymous device information and metadata obtained from both non-users and users to personally identify people, to capture their discrete locations, and to derive their patterns of movement. And most importantly, Section 4.4.4 does not prevent Alphabet from personally identifying both non-users and users by using other data sources or databases (such as non-EBK databases it owns) to cross-reference unique device IDs that are contained in them. Section 4.4.4 does not prevent Alphabet from giving non-personally identifiable information – such as a MAC Address – to a third party, and then having that third party personally identify the owner of the device through data processing and analysis.

So, because it does not prohibit it, Section 4.4.4 gives Alphabet the right to cross-reference non-user unique device IDs with databases that also may contain the same device ID and personally identifiable information associated with it. Thus, the "anonymous" MAC Address captured by the EBKs from non-users who have their Wi-Fi turned on but who don't use any EBK services can be used by Alphabet to identify the non-user.

Alphabet's EBKs Will Capture the Unique IDs of 100% of Mobile Devices Activated in New York City Because Manufacturers Ship Them with Wi-Fi Enabled Upon New Activation

Alphabet is likely to capture close to 100% of the unique device IDs of mobile devices - and their geographic locations - by virtue of the fact that they are configured at the factory to have Wi-Fi enabled when they are activated for the first time. (The same is true for most computing devices today, including laptop and desktop computers, as well as Internet-capable electronics and appliances).

In order to de-activate the Wi-Fi, a user must manually go into their phone's Settings screen and turn it off. Since the vast majority of people don't do this immediately after activating a new phone, or even at all, there is close to 100% probability that their cell phone's unique device ID (MAC Address) will be picked up by an EBK located outside their residence immediately upon activation. And even if they did turn off Wi-Fi immediately upon new activation, it is likely the EBK closest to their building already will have captured the unique device ID anyway. The result is that Alphabet will know the following:

- 1) that a new unique ID (MAC Address) exists, which means a new mobile device exists,
- 2) that it was picked up for the first time by one of its EBKs at location XYZ,
- 3) that since this is a unique device ID that's been recognized for the first time, the person who owns the phone lives on the same block or in the building on where EBK "XYZ" is located (because most people activate their devices at home).

So, from the act of activating a mobile phone (or any other Internet-capable device), Alphabet captures important data that it can use in generating higher revenue from digital advertising.

Randomized MAC Addresses Might Not Be Implemented In A Way To Allow Continuous Anonymity

It is possible for some mobile devices, like cell phones, to generate multiple unique IDs in order to provide a higher level of privacy. This is called MAC Address Randomization and it's dependent on device manufacturers and device operating system vendors (like Alphabet with its Android operating system) integrating this capability into their mobile devices and/or operating system software. This randomization concept has admirable goals, but the devil is in the details of its implementation to assess its effectiveness. (Also see the Monopoly and Anti-Competition section of this document for a discussion on how Alphabet can use its market dominance and power to prevent MAC Randomization from being used in mobile devices running its Android operating system).

If a manufacturer does not allow the randomization to occur within a mobile device in certain operating states, then the feature could be useless. For example, in a September 25, 2014 article in the Washington Post called "Apple's New Feature to Curb Phone Tracking Won't Work if You're Actually Using Your Phone", reporters Ashkan Soltani and Hayley Tsukayama wrote the following on Apple's announcement that it was adding MAC Layer randomization to the iPhone 5:

"The highly praised privacy function [MAC Layer randomization] in Apple's latest operating system that is designed to thwart tracking may not be as effective as originally thought, according to a new post from Bhupinder Misra, a principal systems engineer of the Wi-Fi analytics firm AirTight Networks."

"According to Misra, most iPhone users won't benefit from the feature, which is only active when users have disabled all location privacy sharing and their phones aren't in use. That significantly narrows the likelihood that users will use this feature, he said. If, for example, you wake up your phone to send a text message or check Twitter, your phone will still broadcast the unique code -- known as a MAC address -- as normal, even when you're using your carrier's data connection and not Wi-Fi."

"If you're using the phone, it doesn't randomize," he said in an interview with The Post. "It's only randomizing if the location services are off and [the phone] is in sleep mode. There's only a small percentage of people who would do that."

The Stop LinkNYC Primer

“In his post, Misra also said that the randomization only appears to work with newer devices running iOS 8 -- the iPhone 5s and 5c. He has not yet had the opportunity to test Apple's newest phones, the iPhone 6 and iPhone 6 Plus.”

And from Misra's own blog: *“And then something hit me and it is even more ridiculous (damning) than the earlier finding that location services should be OFF for random MAC addresses to show up. It has to do with the cellular data connection setting. Basically, if the phone's cellular data connection is ON, there is no MAC randomization! If you now turn OFF the cellular data connection (Settings -> Cellular -> Cellular Data OFF), random MAC addresses show up.”*

“Bottom line, this further shrinks the population which is covered by MAC address randomization, perhaps to inconsequential levels and maybe even zero. Who turns OFF location services AND turns OFF cellular data connection while using their iPhone. That is why I now call it “iOS8 MAC RandomGate”.

In addition, in 2017, researchers at the US Naval Academy did a study on MAC Randomization in Android and iPhone mobile devices and concluded that it does not work - they were able to "track 100 per cent of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames." The researchers also state that, "the overwhelming majority of Android devices are not implementing the available randomization capabilities built into the Android OS".

The point here is that while proponents of EBKs may point to MAC Address Randomization as a way to mask the true identity of a user's mobile phone, it is not part of the IEEE 802.11 standard (or the Wireless Broadband Alliance's Hotspot 2.0 standard) – it is dependent on how mobile device manufacturers and operating system vendors implements it. Also, if Alphabet doesn't want its Android operating system to support it, then it would be impossible for a device manufacturer to support it as well (See the Monopoly and Anti-Competition Section of this document for further discussion). To summarize, MAC Randomization may not work under the following circumstances:

- 1) a device manufacturer doesn't support it in its hardware device or its firmware,
- 2) a device manufacturer supports it but makes it difficult to enable or use,
- 3) Alphabet doesn't support it in its Android operating system,
- 4) Alphabet supports it but makes it difficult to enable or use.

The Hotspot 2.0 Wi-Fi Specification Creates Additional Tracking Issues

The Wireless Broadband Alliance (WFA) has created a second generation Wi-Fi standard called Hotspot 2.0 and the Franchise Agreement requires the EBKs to support it. This standard promises to make connecting to public Wi-Fi spots easier as well as to provide benefits for commercial establishments seeking to data mine the Wi-Fi access points they own. One of the main benefits to users is that it allows someone to stay connected to multiple Wi-Fi access points (like the EBKs) as they move around by logging into only one of them, instead of logging into each one they pass. This feature is very suitable for the EBK network since people can walk or drive throughout NYC and maintain constant Wi-Fi service by only logging into one of the units. But, this new standard raises some privacy issues:

Time-Out Period: The Hotspot 2.0 specification does not specify a point in time when someone's device should be disconnected from a Wi-Fi hotspot (like an EBK) after a period of inactivity; this is left up to the wireless access point hardware that's used to provide the Wi-Fi service. If a user connects to an EBK to have a conversation with someone while walking for, say, 20 blocks, and then hangs up without logging out of the Wi-Fi service, the EBK network will continuously capture their personally identifiable information as they make their way through the city unless Alphabet has programmed its EBKs to automatically log out the user after a period of inactivity.

The Stop LinkNYC Primer

If Alphabet chooses not to do this, the company will track the person's device, along with their identity, wherever they go. Since the user had to provide personally identifiable information to log into the EBK network, Alphabet will be able to personally identify the individual's movements and locations even though they are no longer using the EBK Wi-Fi service.

Out-of-the-Box Automatic Hotspot 2.0 Enablement – Similar to the situation where a mobile device's Wi-Fi feature is configured at the factory to be automatically enabled upon new activation, it may be possible for manufacturers and the owners of mobile operating systems to have the Hotspot 2.0 standard support automatic Wi-Fi enablement after the device is newly activated. If this can be done, then it may be that people could be logging into the EBKs against their will with their log in credentials and personally identifiable information. And unless Alphabet logs them out after a period of inactivity, it will be able to track, locate, and personally identify the individual wherever they go in the city, **without their knowing it**, down to the block or building, 24/7/365.

The Franchise Agreement Does Not Define “Anonymized Aggregated Data” (AAD)

The Franchise Agreement refers to “anonymized aggregated data” (AAD) but does not define what it is. This means that Alphabet and the City can define what this term means and the types of data that fall under it without any input or oversight from the public. A major question for the people of New York is whether anonymized aggregated data includes unique device data such as telephone number, Medium Access Control address (MAC address), IP address, device Wi-Fi name, the specific EBKs the devices have connected to, EBK connect and disconnect date, and EBK connect and disconnect times. Another question to be answered is whether any of the AAD is linked to unique device IDs (MAC Addresses). If the City is receiving this information (for example, under section 3.12.5 in the amended Franchise Agreement as of September 9, 2015, then it would have a record of the location, time, and date of every mobile device that has its Wi-Fi turned on, and it would have the ability to personally identify the owners of the devices for which it has the unique device IDs.

The City could request all this information for just one unique device ID (for example, one specific cell phone), claiming that it is anonymized aggregated data since it doesn't know who owns the device. But this would not prevent the City from cross-referencing this unique device ID data with other databases to which it may have access (or can rent or purchase) and which contain both the ID and personally identifiable information associated with it.

The Supreme Court's June 2018 decision in Carpenter v. United States renders the City's to obtain this data unconstitutional. A public hearing should be held to determine the definition of anonymized aggregated data and whether the City should have access to it. At minimum, a coalition of privacy rights and civil rights groups needs to work with the City to define what it is. In addition, the City needs to publish in what form it will receive the data. It also needs to be required to publish each time it 1) receives anonymous aggregated data from Alphabet, 2) what that data is, 3) whether specific MAC Addresses – or other unique IDs such as an IP Address or advertising IDs - have been singled out as part of its aggregated anonymous data collection, storage and analytics processes, 4) what the specific MAC Address and other unique IDs are, and 5) whether it has associated personally identifiable information to it.

EBKs Will Capture Home Wi-Fi Router and Home Personal Computer Unique IDs and Names

A major privacy issue that is raised by the EBKs involves home Wi-Fi routers and home personal computers that have Wi-Fi enabled. For people living in range of the EBKs, which is currently 150 feet in both horizontal and vertical directions (and possibly up to 400 feet), the unique router ID, the name of their home Wi-Fi networks, and their Wi-Fi-enabled home personal computers and other Wi-Fi devices will be captured by Alphabet. This means that one company, Alphabet, will know where the home routers and computing devices are located throughout NYC down to the block or building. It will capture this information for both residential and commercial units since Wi-Fi signals go through building walls. **So, in addition to one company – Alphabet - knowing the unique device IDs of every mobile device in the New York City, it will also be the only company to know the unique device IDs**

(MAC Addresses) of every Wi-Fi enabled device or product in homes (as well as commercial establishments), including home routers, home computers and Wi-Fi-enabled televisions, appliances, and other products.

Why Alphabet Wants to Capture Unique IDs of Home Routers and Computing Devices

In the beginning of this document, an overview of Alphabet's business and revenue model was provided. To summarize, Alphabet makes 90% of its revenue through digital advertising fees. It uses unique device IDs, other device metadata, and personally identifiable information – and other data - as key assets to provide targeted advertising for which it charges fees and in many cases, premium fees to its advertisers...the more personal information it can provide to an advertiser about someone, the higher the fees it can charge. The EBKs enable Alphabet to identify all home computing and networking devices down to the block or building since they are able to capture their Wi-Fi signals. By knowing the exact location of home router and computing devices, it can provide better targeted ads for its advertisers and thus can charge higher fees for its own advertising platform, AdSense, as well as through 3rd-party advertising platforms it uses. Also, it could provide more targeted ads for companies advertising on its EBKs since it knows the geographic location of all devices and computers in New York City. By analyzing where all these devices are (home computers) or travel (mobile devices), Alphabet could provide a high level of targeted advertising for which companies would pay a higher premium. Prior to the EBKs being deployed, Alphabet couldn't do this. The closest the company could ascertain the location of a home computing device, a mobile device using the home's router, or the home router itself was knowing where a broadband Internet provider's routers were located, such as those owned by Verizon FiOS or Spectrum. But now with its network of EBKs, it knows the exact block or building where the home computer, mobile device or router is located. And by knowing the location of these devices at the block and building level, Alphabet has the ability to charge higher fees to its Web and EBK advertisers.

Alphabet can – without device owner authorization - turn on a device's Wi-Fi service in order to have its EBKs locate where the device is, and by extension locate the block in New York City where the person who owns it lives.

Alphabet has the ability to turn on the Wi-Fi of a device without the owner's authorization. It would want to do this – and already has – in order to 1) locate where a person lives in New York City and 2) to track the device and owner throughout New York City. In 2018, Alphabet turned on the Wi-Fi of Android phones in Manhattan in the dead of night when everyone was sleeping. One Android device owner, who never uses Wi-Fi and keeps it disabled and who always puts the device in airplane mode before going to sleep had their phone turned on by Alphabet sometime between 11pm and 7am. When the person awoke in the morning, they had a message on their phone from Alphabet that that said "Free Wi-Fi available in your area", and the device's Wi-Fi had been turned on. When the individual looked at the Wi-Fi networks available they saw that LinkNYC was in the list. The message sent by Alphabet must have been done through some notification capability (it was not a text message) in the phone that does not require cell, Wi-Fi, or Bluetooth service to be enabled. Or perhaps Alphabet was somehow able to first turn on the device's Wi-Fi through a software program installed through a previous software update, and then send the message. It is clear that Alphabet did this in the dead of night in order to pinpoint the block where the owner of the device lives....99.99% of people are sleeping at home at 3am in the morning. By turning on the Wi-Fi of Android devices in the dead of night throughout all of Manhattan, Alphabet was able to obtain the block location of where the owners live. This type of information is very valuable to Alphabet since it gives the company demographic information about peoples' economic status, which it can use to sell advertisements via its EBK advertising, as well as through its other web services. No doubt, Alphabet will continue to do this unethical and illegal activity as the EBK network continues to be deployed and in perpetuity. In addition to this creepy invasion of privacy, Alphabet is illegally controlling the private ownership of a user's device. There is nothing in any user agreement that would allow Alphabet to turn on a user's Wi-Fi without their permission. And since the City of New York is the de facto majority shareholder of the company (given that it gets a majority of its revenue), it also is violating peoples' privacy and illegally controlling their devices.

Alphabet Might Be Violating Federal Wiretaps Laws with its EBKs in Light of the 9th Circuit Court of Appeals Ruling in Google v. Joffe, et al, No. 11-17483

In 2013, in Google v. Joffe et al, 9th U.S. Circuit Court of Appeals, No. 11-17483, Google (Alphabet) was found guilty of federal wiretap laws because it equipped vehicles used for its StreetView mapping business with “electronic snooping” technology to capture the messages, unique device IDs, and other metadata of private citizens’ communications from their home computer networks and home computers. The data Google captured were the content of emails and Web pages, unique device information such as MAC Addresses, passwords, and router network names. The court ordered Google to stop the practice, delete all information it had stolen, and pay a fine. With its EBK Wi-Fi network, Alphabet is doing the exact same thing that it was found guilty of with its Streetview mapping program as it relates to people who don’t use the Wi-Fi service but who have Wi-Fi turned on in their mobile devices. This court case illustrates Alphabet’s desire to collect as much information about people’s technology networks and device IDs so that they can include them in their database profiles of devices (unique device IDs) and the people who own them. The “electronic snooping” it engaged in had nothing at all to do with its StreetView mapping business. It was something the company did in order to get as much information about peoples’ devices so it could use the data to increase its revenue.

This court case is raised here because what Alphabet could not achieve illegally through its StreetView mapping effort – that is, collect unique device IDs and home router SSIDs and – it is achieving at the blessing and authorization of the City of New York. Essentially, Alphabet and the City are violating federal wiretap laws by making an end run around the 9th U.S. Circuit Court of Appeal’s ruling which determined Alphabet was guilty of violating them through StreetView because people had not legally consented to having their electronic communications and device metadata captured by Google. Now, instead of using its StreetView vehicles to capture unique device IDs, router SSIDs, and other metadata, Alphabet is using its government-granted monopoly to do the exact same thing with its LinkNYC EBK units. **The legal authorities, consumer watchdog groups, civil rights groups, and privacy rights groups who received this document should investigate Alphabet’s use of its EBKs to capture unique device IDs, home router SSIDs and computer metadata in the context of the 9th U.S. Circuit Court of Appeal’s decision.**

Alphabet Will Be the Only Company in New York City That Will Possess Metadata on all Wi-Fi-Capable Mobile Devices, Computing Devices, Electronic Products, and Home Appliances

The EBK network is unique from all other communications networks in New York City in that it is the only one that will capture MAC Addresses and other metadata from all Internet-capable Wi-Fi devices. No other wireless (that is, cell phone) carrier or wireline carrier can do this since their networks are either dedicated to specific devices (like cell phones) or are technically not able to do so (like cable companies). Alphabet, then, is the only company in the New York City market that will be able to capture MAC Addresses (unique device IDs) and other metadata from all devices and products including the following: cell phones, tablets, personal computers, digital music players, Wi-Fi-enabled home appliances, Wi-Fi-enabled televisions, Wi-Fi-enabled vehicles, and any other Wi-Fi-enabled consumer product.

The number of MAC Addresses and the amount of metadata that Alphabet will capture through its EBK network is massive; it is unparalleled in the history of digital communications. Alphabet will be the only company to know all the Wi-Fi devices and products that exist in New York City as well as know their locations at all times, down to the block or building, 24/7/365. It will be the only company that can track all mobile devices and products in the city at all times. That it’s the only company who will possess all of this information gives it incredible power over people as well as over its wireless, wireline, and Web competitors (see Monopoly and Anti-Competition Section). Moreover, all of this information can be obtained by the City of New York. While the City claims it will receive only anonymized aggregated data, there is no public definition of what that is, which means the City could get specific MAC Address and other unique identifiers on devices and then conduct analytics to personally identify the owners.

Alphabet's Privacy Policy Allows it to Track Minors Throughout the City

Alphabet's EBK network cannot distinguish between Wi-Fi-enabled mobile devices owned by adults and minors. This is true for devices that have both cell and Wi-Fi capability and those having only Wi-Fi capability (like digital music players, tablets, etc). Since the Franchise Agreement does not prevent Alphabet from doing analytics on device metadata, the company can track and follow minors. The company is able to do this because each EBK in the city can capture and then send to a database server the unique ID of devices used by minors. Alphabet can run an analytics software program that compares the EBK database data against other databases that contain the same device ID and a minor's personally identifiable information such as first name, last name, birth date, age, social security number, address, etc. For example, the Google Gmail database that has a minor's personally identifiable information and their MAC Address (while Alphabet states in its privacy policy that minors under the age of 13 cannot use EBK services, there is no way it can prevent this). Moreover, since the City allows Alphabet to offer its EBK services to minors between the ages of 13 and 18, it is aiding and abetting Alphabet's tracking of this population.

In addition to any existing information Alphabet has about minors in its databases it will capture new information, such as where they go to school, since EBKs are located next to them. By using analytic software programs, Alphabet could determine the school a minor goes to as well as the time of arrival and departure since the EBKs will pick up their device's unique ID when arriving to and departing from it. Alphabet also will know the route minors walk and ride home since its network of EBKs will capture their unique device IDs along the way.

There are no technical or operational ways that Alphabet can prevent its EBK network from capturing device data from minors, or from their using the service.

So, unbeknownst to minors (and their parents), Alphabet will know their location at all times and can track them wherever they are in the City, including knowing the schools they attend and the routes they travel. This is true for minors who are either non-users or users of its EBK services.

The City of New York Might Have Approved the Deployment of a Free Wireless Broadband Network with the Ulterior Motive to Install a Massive Tracking and Surveillance Network

Because the City has allowed Alphabet to deploy a wireless broadband network that also includes various technologies that will be used to record people in their daily activities outside and inside their homes, it's quite possible that the City's ulterior motive for approving the deployment of the EBK network in the first place is due to its desire to track people through a massive video and audio surveillance network.

Consumer watch dog groups, digital privacy groups, civil liberties groups, as well as legal, regulatory, and legal authorities at the State and Federal levels should initiate an investigation into the following:

- 1) the need for free wireless broadband in the City. The City claims that "over 25% of New Yorkers lack high-speed broadband", but it doesn't define what that means. Neither the City nor Alphabet cite 3rd-party, independent, statistically significant data that supports this number (see Footnote below).
- 2) Does the "over 25%" claim mean that this population wants broadband service but can't afford it or get technical access to it? Or does it mean they don't have it and don't want it but can afford it?
- 3) Does the figure include people living in the country illegally? The City should NOT be including - as partial justification for a non-critical, non-utility infrastructure project like the EBK network - illegal immigrants living in the city (which some estimate to be between 500,000 and 900,000). This population is a material percentage of the 2 to 2.5 million people the City and Alphabet claim don't have access to broadband service. Specifically, at the low end it is 20% of the total and at the high end it is almost 50% of the total.
- 4) what capabilities were discussed during the wireless broadband public hearing or administrative process,

The Stop LinkNYC Primer

- 5) whether non-communications capabilities, such as video recording and audio sensors and recording, were discussed during the hearings or administrative process,
- 6) if non-communications capabilities were not discussed, then how did they make their way into the EBKs,
- 7) did the inclusion of non-communications capabilities violate the law,
- 8) did the inclusion of capabilities that can monitor and track people violate existing statutes as well as the U.S. Constitution's 1st, 4th, 5th, 9th, and 14th Amendments,
- 9) who was involved in this effort and what were the communications between the City and Alphabet that resulted in non-communications capabilities being included in the EBKs.

Footnote for #1: many elderly people, who comprise a fairly large percentage of NYC's population, do not want to use the Internet for a number of reasons including: a) they are not interested in it, b) they don't use computers or mobile devices, c) they physically are unable to use computers or mobile devices due to poor eye sight, loss of dexterity, or neurological disorders, and d) they are mentally incapacitated due to serious medical conditions. These people may have technical access to broadband but simply don't want it for any of the aforementioned reasons. And to reiterate, illegal immigrants cannot be included in the population that lacks broadband access because they are not supposed to be in the country in the first place. Lawful residents and citizens are not responsible for providing free broadband Wi-Fi to illegal immigrants. It is a non-utility, non-critical, discretionary communications service.

Integration of Video and Photographic Capabilities in EBKs Violates the Franchise Agreement

Alphabet states in its Privacy Policy (as of January 2016) that the EBKs can record video and "sense" audio. It is assumed that through its audio sensing feature and/or the external directional speaker, the EBKs also can record true audio (e.g. conversations from the streets), as well as take photographs through the video camera. **The Franchise Agreement, however, does not allow Alphabet or the City to include video recording, audio recording, image capture, or environmental sensors....yet every EBK has these capabilities. This is a clear violation of the Franchise Agreement, which specifies that the EBKs can provide only broadband Internet service to Wi-Fi devices, voice communications from the interactive screen, battery re-charging, and display electronic ads.** If one searches on the terms video, audio, or photograph in the Franchise Agreement's "Services" section (Attachment SRV), not one instance of any of these words can be found. In the main Franchise Agreement document, the only references to audio are with respect to advertising and playing audio in the context of the provision of telecommunications services (presumably broadcasting audio externally through a speaker).

The fact that none of these four capabilities is included in the Franchise Agreement begs the question as to whether they were discussed during the public hearing process which resulted in approval of the EBK wireless network. The City needs to prove that these capabilities were part of the official administrative and/or public hearing process. **If it can't do this then these capabilities physically must be removed – not just disabled – from every EBK.** These capabilities have absolutely nothing to do with providing broadband Wi-Fi service, which the Franchise Agreement specifies as the sole reason for having the network in in the first place.

If the City included or allowed technical capabilities that were not part of the City's process for approving the Wi-Fi broadband service - or necessary to the provision of the service - it has violated the law and the Franchise Agreement.

The main Franchise Agreement document addresses the allowed services in a general manner in Section 4.1.1: *"4.1.1 is intended to provide a summary of the Franchisee's obligations and is not intended to modify or supersede the scope of the Public Communications Structure Services described in Attachment SRV.*

(i) Assume ownership of all Existing PPT Systems.

(ii) Design, install, operate, and maintain the System, including the replacement of Existing PPTs with New Structures.

(iii) Provide free or pay telephone service.

(iv) Provide free public Wi-Fi."

The Stop LinkNYC Primer

Attachment SRV provides more detail about what the EBKs' Public Communications Structure Services are, **and it does NOT include any video, photographic, or audio recording or sensing capabilities.** The sections of the SRV Addendum relating to this are:

3.3 Telephone Service Features

All Structures built after the Commencement Date must provide the following: telephone service via touch screen, integrated lighting, directional speakers, a tactile key pad and braille lettering, a dedicated 911 button, and a USB charging port.

4.1.3 "Users" means people making use of the Wi-Fi Services.

4.1.4 "Wi-Fi Equipment" means the hardware, parts, systems, and components necessary to provide the Wi-Fi Services.

4.1.5 "Wi-Fi Service(s)" means the provision of continuous, uninterrupted, unrestricted, free Wi-Fi (wireless fidelity) service, or similar wireless service of comparable use approved by the City, to Users of the internet on Wi-Fi enabled devices.

4.2 General Description of Services

4.2.1 All PCS's, other than Existing PPTs, must provide free Wi-Fi Services in accordance with the requirements of this Agreement, including Part IV, and must be capable of supporting up to 256 devices with a total aggregate throughput of 1Gbps. Franchisee shall provide the Wi-Fi Services twenty-four hours per day, seven days per week, 365 days per year throughout the term of this Agreement, with an uptime of at least ninety-seven percent (97%) exclusive of upgrades and planned maintenance providing at each PCS a Wireless Access Point (WAP) supporting simultaneous dual spectrum 2.4 GHz 802.11 b/g/n, and 5GHz a/n/ac services.

4.2.2 The Wi-Fi Services must provide a signal strong enough to create a Wi-Fi hotspot that extends a one hundred and fifty (150) feet in line-of-site, regardless of traffic conditions, measured radially from the center of the Structure. A User must be able to log in once and stay connected while within one hundred and fifty (150) feet in line of site of any PCS. The Wi-Fi Services will be able to allow the Users' devices to automatically re-connect after a connection has been severed and the User comes within the range of another Structure.

It is crystal clear from the Franchise Agreement and its addendums and exhibits, which describe the required – and restricted - features and capabilities for broadband Wi-Fi communications service, that the EBKs are NOT allowed to contain video, image capture, audio recording or audio sensing capabilities. These capabilities have nothing to do with the provision of Wi-Fi communication services, which is the only thing the Franchise Agreement allows Alphabet to engage in (as well as digital advertising and voice communications).

State and Federal Legal Authorities Need to Conduct an Investigation on How EBK Non-Communications Capabilities Were Integrated into the Units

State and Federal government authorities need to conduct an investigation into how video recording, audio recording, image capture, and environmental sensing capabilities were included in the final EBK product, whose only purpose – as defined by the Franchise Agreement - is to display electronic ads and provide broadband Wi-Fi service to Wi-Fi enabled devices, and voice telephone service. Clearly, the integration of these capabilities was not done by accident. There must have been communications about these unauthorized capabilities between the City and Alphabet outside of the public hearing process since they are not mentioned at all in the Franchise Agreement or its various addendums and appendices.

The Stop LinkNYC Primer

Some of the questions State and Federal legal authorities need to ask are the following:

- 1) At what point were capabilities not included in the Franchise Agreement first talked about between Alphabet and the City (i.e., video and audio recording, audio sensing, and photography)?
- 2) Why were these capabilities not included in the public hearing process?
- 3) Why were these capabilities not included in the Franchise Agreement?
- 4) Why were these capabilities mentioned in Alphabet's privacy policy as of January 2016 but not sooner in any City legal documents or other documentation?

The Inclusion of Video Recording, Audio Recording, Audio Sensing, and Photographic Capabilities in the EBKs is an Invasion of Privacy.

The integration of video, audio, audio sensing, and photography into the EBKs is a gross violation of peoples' right to privacy. The video camera is embedded in the EBK's display panel and is located at the top and center of the unit. Alphabet was very deliberate in the way it designed the camera so that it would not be detected by people unless under very close inspection; and even then it is difficult to tell it is a camera. The camera is situated about eleven (11) feet above the ground. Nobody would notice it with just a cursory look up as they walk by an EBK; those biking or driving by would never even have the opportunity to see them. One has to be close to the unit and focus on the dark circular spot (which contains the camera) in order to see something inside; and even then one can't really tell it's a camera.

The EBKs are designed with concealed video cameras because Alphabet and the City do not want people to see that they are being video recorded and photographed everywhere they go. In addition to the concealed nature of the video monitoring and recording, there is no information on the EBK itself stating that it can do so, and there are never any notices on the display screens saying the same.

The City must have wanted the video cameras to be concealed since having 20,000 external cameras mounted on top of 10,000 EBKs would have raised many concerns and complaints about personal privacy. That is to say, the appearance of two external cameras on each of the 10,000 EBKs facing opposite directions would have instigated an uprising on the part of New Yorkers. The City must have approached this concealed design with a "what you can't see can't hurt you" philosophy. How different the EBKs would look if they contained external cameras the size of the typical NYPD surveillance camera, and how different New Yorkers would react to the massive number of them. And Alphabet also probably did not want to design its EBKs with external surveillance cameras primarily because of fear of political backlash. At least with NYPD cameras, you can see them and there are signs saying that the area is under video surveillance. This is not the case with Alphabet's EBKs; you can't see the video cameras and there are no such messages on the units stating that the electronic billboards may, or will, video record or photograph you without you knowing it. And there is no indication to anyone when the cameras are in operation. (The same issue is true about EBK audio recording and sensing capabilities, which are addressed in the next section).

The ability to video record people on virtually every block of the city has profound privacy implications since people do not know that:

- 1) They are being video recorded and/or photographed.
- 2) They are being video recorded and/or photographed virtually everywhere they go in NYC.
- 3) Alphabet and NYC can track their whereabouts down to the block or building via facial, picture, and pattern recognition.
- 4) Their MAC Addresses can be combined with video/photos taken by the EBK, which would allow the association of their MAC Address to their personal likeness.

Surveillance Recordings Would Not be Allowed by the City or the People if Government Employees Were on the Streets Using Video Cameras or Audio Recorders

The City would not allow either its own staff or Alphabet's employees to video or audio record the public with handheld devices, and the public would not accept it either. Imagine that instead of the two concealed EBK cameras that are embedded in each structure, Alphabet and/or the City had two employees located at each EBK installation with video cameras recording people, 24/7/365. Nobody would put up with such an incredible intrusion on privacy; it simply would not be approved by the City, and it would be totally rejected by the people. But this is exactly what the City and Alphabet are doing...but just in a secretive way via the concealed EBK video cameras. **That the cameras are hidden and are not manually held by Alphabet or City employees does NOT make it acceptable to have them.**

Alphabet and the City Can Record Audio Throughout New York City

Similar to video recording, the same is true with the audio recording capability of EBK external speakers, which are used by those who make telephone calls. Since an EBK doesn't have a telephone handset, its external speaker must be used in order for someone to speak to another person. This means that the external speaker is also a listening device that can pick up conversations from the street. And this means that Alphabet has the technical ability to record any audio it captures from the street (and is probably the reason the City did not want a handset in the units). The same issue applies here as it does with video recording: neither the City nor Alphabet would be allowed to place employees where each EBK is located with handheld audio recording devices. **That the external speakers are embedded in the EBK structure does NOT make it acceptable for the City or Alphabet to record audio from the street.**

Alphabet Can use Facial, Picture, and Pattern Recognition Technology to Determine a Person's Identity

Alphabet is involved in the development and acquisition of facial, picture, and pattern recognition technologies in order to expand its business offerings and increase its advertising and other revenue. It is exploring the application of these technologies in different ways. One of the ways it could use them is to cross reference images of people its EBKs capture with pictures a person may have on websites, such as a social media sites like Facebook, Instagram, Pinterest, LinkedIn, etc. Alphabet does not need to own the website on which an individual's pictures reside; it can use its own "Internet worm crawlers" or third-party companies to do the picture association. From this, Alphabet may be able to identify individuals' names and addresses. Any type of facial, picture, or pattern recognition analysis performed by Alphabet, either on its own at the direction of the City, would be unknown to people. You may be someone who does not want to interact at all with the EBK's, but Alphabet doesn't need you to in order to identify you; all it needs is to capture your face and it may be able to identify you. As the old saying goes, "you can run, but you can't hide" from the all-seeing EBKs.

The reader should be aware that Alphabet is a leading company in the development and use of facial, picture, and pattern recognition technologies, and it continues to grow its capabilities in these areas. For example, in 2016 it purchased a company called Moodstocks, whose technology can recognize what activities are taking place in a picture. You can read more about Alphabet's facial, picture, and pattern recognition at its website, google.com, including in its privacy policy.

Alphabet and the City Have No Published Policy on the Use of Video or Audio Recording, Audio Sensing, or Photographs

Neither Alphabet nor the City has published any information on when video or audio recordings will be made, for what reasons recordings will be activated, or when photographs will be taken. Alphabet's privacy policy of January 2016 states that if it records video, it will keep the video for no longer than seven (7) days. But there is no information in the Franchise Agreement, the controlling legal document for the EBKs, as to the following:

The Stop LinkNYC Primer

- 1) When recordings or photographs will or can be done.
- 2) The length of time recordings can be kept (the City has allowed Alphabet unilaterally to determine this time period).
- 3) Who can authorize the start and stop of recordings.
- 4) Whether people will know they are being recorded or photographed either through messages on the display screen or by a permanent, visible sign affixed to the EBK structure.
- 5) Which EBKs will do recordings.
- 6) The reasons for recording or photographing.
- 7) Who within Alphabet has access to recordings and photographs (network administrators, executives, lawyers, etc.)? Do they have security clearance?
- 8) Who within the City has access to the recordings (DoIT management, NYPD and other law enforcement, City attorneys, IT administrators, DOT managers, DOT administrators, etc.)? Do they have security clearance?
- 9) Whether Federal or State government agencies or legislative bodies have access to recordings and photographs (NSA, DHS, the U.S. Congress, NY State Assembly, the NY State Executive branch, the USDOT, the FCC, etc).
- 10) Which Federal government employees have access to recordings and photographs; and what the titles are. Do they have security clearance?
- 11) Where recordings and photographs will be stored (specific storage devices, whether in flash or on disc drives, locations of storage devices such as internal or 3rd-party datacenters and hot site backup datacenters, if any).
- 12) How recordings/photographs are deleted (e.g. simple delete/recycle, shredded, Department of Defense-level shredded, etc.).
- 13) What the physical and digital security policies for stored recordings are.

Importantly, the Privacy Policy does not cover audio recordings Alphabet can make through remote activation of the speaker that is used for voice telephone calls.

Neither Alphabet nor the City of New York Has Disclosed to the Public Anything About Environmental Sensors Contained within the EBKs

The Alphabet Privacy Policy, as of January 25, 2016, states that “environmental sensors” are installed in the EBKs. It does not define what environmental sensors are or what their capabilities are. The Franchise Agreement has no references to them at all, which means the EBKs are in violation of the contract with the City. The fact that an environmental sensor was built into all EBKs without authorization by the Franchise Agreement begs the question, of course, how did this capability get included and for what purpose.

Alphabet and the City must fully disclose to the public the technical specifications for the “environmental sensors” and what circumstances they will be used for. As part of the technical disclosure, they must say whether this capability can record human conversations from the street. Moreover, the City must explain how this capability was built into the EBKs when it was not authorized by the Franchise Agreement.

The City Has No Provision in the Franchise Agreement to Monitor and Audit Video and Audio Recordings, and Audio Sensing

Since the Franchise Agreement does not authorize the integration of video and audio recording/sensing capabilities in the EBK units, it means the City has no provisions regarding how it is to monitor and audit the recordings. Information that is critical to the public includes:

The Stop LinkNYC Primer

- 1) What video and audio has been recorded.
- 2) The length of the segments.
- 3) The dates they were taken.
- 4) The dates they were deleted.
- 5) The reasons for the recordings.

If there are no reports about any of these things, especially on the deletion of the recordings, then there is no way to get Alphabet's factual and legal representation that the recordings were destroyed. A complete accounting of all video and audio recordings, audio sensing recordings, and photographs must be documented and provided to the City and privacy rights organizations. A complete accounting on when files have been deleted or destroyed also must be documented and provided in a report. Information that must be included in the deletion reports includes: the time and date of deletion, the file identification number or name, method of deletion (e.g shredding), person's name and title who did the deletion, and signature of the person to confirm they were the one who deleted the files. In addition, a periodic report must be provided that compares the files recorded (the file names) by the EBKS to the files deleted (the same file names) so that it can be ensured that all recordings were actually deleted.

The City Has No Technical or Operational Way to Ensure Video and Photographs are Deleted

While the public can demand Alphabet and the City confirm the deletion and destruction of recordings, the fact is that there is no definitive way to ensure this has occurred. Alphabet claims it erases video recordings after seven (7) days but there are no independent technical or operational methods the City can use to confirm this. The City can only take Alphabet at its word that it has deleted video, audio and images. But Alphabet can simply falsify documents that state deletions have been done. There is absolutely no way that the City can ensure that recordings are deleted and no way to challenge or disprove any falsified statement that Alphabet may make. It is purely a matter of faith on the part of the City that Alphabet will delete or destroy recordings. Without a direct operational and technical way to ensure recordings have been deleted, the legal language of the privacy policy is a paper tiger; it means nothing. **That the City has no technical or operational methods to ensure recordings have been deleted is reason enough to forbid Alphabet from engaging in this activity through its EBKS.**

EBK Cameras Can See Inside Apartments and Violate the Right to Privacy in Domiciles

The EBKS have their video and photographic cameras directed at peoples' apartments. The illegality of Alphabet and the City deploying cameras that can see inside domiciles is obvious; neither of these entities has the legal authority to videotape or photograph people inside their private residences. Questions that need to be answered by Alphabet and the City are:

- 1) Do all the EBKS have the same camera hardware and software?
- 2) If different camera hardware and software are used in the EBKS, why is this?
- 3) What is the field of view of each camera? (that is, can the cameras see 180 degrees up and down and 180 degrees from side to side?)
- 4) What is the resolution of each camera?
- 5) Can the resolution of the cameras be made higher through software upgrades or do they need to be physically replaced?
- 6) Can the cameras zoom, and if so, what is the magnification?
- 7) Can the direction of the camera be moved, either manually at the EBK unit itself or remotely via computer?
- 8) Has the City tested **each** of the two cameras installed in **each** EBK to determine whether they can see people or objects in apartments? (this must be done by the City, not Alphabet).
- 9) Do the cameras have infrared capability so it can see and record at night?
- 10) What is the testing methodology the City has used to ascertain whether **each** EBK camera can see inside peoples' residences?

The Stop LinkNYC Primer

- 11) How has the testing been documented for **each** EBK?
- 12) Does the City have a verification process to ensure that only certain types of cameras (hardware and software) are used?
- 13) Does the City have a policy on how camera hardware and software are updated or upgraded?
(The appropriate process would require Alphabet to submit any changes to cameras through a public board comprised of individuals from the City, civil rights organizations, digital privacy organizations, and independent technical consults who have no previous or future business/commercial interests with Alphabet or the City.)

Other Intrusions on Privacy by EBK Video, Audio, and Photographic Recording Capabilities

Ascertaining Personal Relationships through Video Recording

With facial, picture, or pattern recognition, Alphabet can identify people with whom one associates. By capturing video or images of a person and, say, their significant other or business associate, the company could compile a profile of the people that the person knows and with whom they spend time, as well as their locations. All of this would be done without people knowing this is happening and without their consent.

Intrusion on Personal Lives

The personal lives of people will be compromised by the EBKs' video recording and photographic capabilities. Every single act a person does on their own or with others in NYC can be recorded and stored without their consent. Neither Alphabet nor the City has a legal right to do this under existing statute or Constitutional law.

EBK Video and Audio Recording Capabilities are Un-Constitutional, a Threat to Liberty, and Can Suppress Political Speech.

The same Constitutional issues raised earlier in this document - by EBKs capturing unique device IDs (MAC Addresses) - are raised with video and audio recording capabilities (see Sidewalk/Intersection's January 2016 Privacy Policy for information related to EBK video recordings). Specifically, 1st, 4th, 5th, 9th, and 14th Amendment issues are raised by the video and audio recording capability, which will be done on virtually every block of the City by 10,000 EBKs.

The EBK network will stifle political speech and dissent of people who do not want to have their activities and participation in political events/activities video and audio recorded by Alphabet and the City; they will choose not to participate for fear of being tracked by the government and then, potentially, met with reprisal. Alphabet may be able to conduct facial, picture, and/or pattern recognition on people and use that information to cross reference with other information it has on the individual to personally identify them.

In addition, Alphabet and the City can also use a mobile phone's unique device ID (MAC Address) to identify those involved in political protests/rallies by using it with facial/picture/pattern recognition databases they own which contain MAC Addresses and personally identifiable information. The City, if it does not own this information itself, can simply contract with Alphabet or other commercial companies to use their databases to match MAC Addresses, and pictures of faces.

Alphabet's Privacy Policy Regarding Facial Recognition is Not Technically or Operationally Enforceable, is Not Auditable, And Does Not Include Picture or Pattern Recognition

Alphabet's privacy policy states:

We will not use facial recognition technology for any reason, and we will not use our cameras to track your movement through the city.

The Stop LinkNYC Primer

While this is a laudable statement, the fact is – like with the deletion of video recordings and images - there is no technical or operational way that the City can prevent Alphabet from using facial recognition and using it to track movement throughout the City. The City, again, must rely only on faith that Alphabet will not do this; it has no technical or operational mechanism to audit whether Alphabet is using facial, picture, or pattern recognition and whether it is using it for tracking purposes. The only way the City would be able to find out if the company is violating this provision of the Alphabet privacy policy is if: 1) an Alphabet internal document about it becomes public, or 2) an Alphabet employee reveals it to the public or to private persons or government officials. Moreover, the above statement only covers Alphabet because it uses the word “we”, which refers to the company itself...it does not cover the City. So, the Privacy Policy allows the City of New York to use facial recognition and to use the cameras to track people throughout New York City.

Alphabet’s Privacy Policy Does Not Address the Use of Picture or Pattern Recognition

Alphabet’s privacy policy does not include a prohibition against using picture or pattern recognition to identify and track people. Picture recognition uses non-facial data points to identify and track individuals; for example, someone’s hat, a piece of jewelry, a t-shirt slogan, or red jacket. Pattern recognition uses movements in video to identify people (or objects) and track individuals. While there are overlaps with facial, picture, and pattern recognition, there are distinct differences among them.

To reiterate, in 2016 Alphabet announced it would purchase a French company called Moodstocks for its pattern recognition technology. Clearly, this is another visual recognition capability that Alphabet is developing and both it and picture recognition need to be prohibited by the Privacy Policy.

There are No Financial or Criminal Penalties if Alphabet or the City Violate the Privacy Policy

The City does not state in the Franchise Agreement whether there are penalties for Alphabet’s violation of its Privacy Policy. Without severe financial, criminal, or other penalties the privacy policy is simply toothless. The City must create a policy that levies severe fines on Alphabet and its employees, as well as criminal punishments, if it violates any part of the Privacy Policy. These penalties must be included in the Franchise Agreement. In addition, there also must be penalties for City employees who violate the Privacy Policy.

Without severe penalties for violating the Privacy Policy, Alphabet can engage in activities prohibited by it with impunity. If the City finds out the company has violated the privacy policy, there is no mechanism to punish the company or its employees. Simple warnings and threats by the City to do “this or that” are: 1) not legally enforceable, and thus 2) not an effective punishment against Alphabet for violating the privacy policy. **The bottom line is this: the Franchise Agreement does not provide for any punishments that would prevent Alphabet from engaging in activities prohibited by its privacy policy. It also does not provide any punishments against City employees who do the same.**

It must always be remembered that Alphabet monetizes the data it gets from the EBKs. By violating the Privacy Policy, Alphabet could generate more revenue for itself. Because of this potentiality, financial and criminal penalties must be established and contained in the Franchise Agreement, and they must be severe in order to act as a deterrent. And it also must be remembered that the City and Alphabet are business partners, where the City has a financial incentive to grow Alphabet’s business as much as possible since it reaps a majority of revenue starting in Year 8 of the contract. **Because of this percentage-based financial model, the City is also incented to compromise the public’s privacy either through a weak Privacy Policy or by allowing Alphabet to violate it.**

The City Has Failed the Public by Allowing Alphabet, And Not the City and Public, to Create the Privacy Policy for NYC Residents

In what is clearly an enormous giveaway to Alphabet, the Franchise Agreement allows Alphabet - not the City - to create the Privacy Policy around all of the data collected by the various capabilities, features, and services of the EBKs. **The City has done the exact opposite of what it should have done.** The City should not allow a private company to determine the Privacy Policy for the public on whom it relies for its monopoly franchise and from

The Stop LinkNYC Primer

whom it is using public lands – the sidewalks. The privacy issues raised by the deployment of the EBKs on such a massive geographic scale – along with all of their data collection capabilities – **demands that the Privacy Policy be created by the public and forced upon Alphabet as a condition of being the monopoly franchise.** The types of organizations that need to be involved in the creation of the privacy policy include, but are not limited to, the following:

- 1) Civil Rights organizations
- 2) Digital Privacy organizations
- 3) Consumer Watchdog organizations
- 4) Government Watchdog organizations
- 5) Motorist trade associations
- 6) The City of New York's Corporation Counsel, Human Rights Council, Department of Information Technology, Department of Transportation, NYC Community Boards, the NYC Council
- 7) New York State legislative and executive branch bodies and departments
- 8) U.S. Justice Department
- 9) U.S. Department of Transportation

Without a privacy policy board comprised of entities and organizations that represent the public's right to privacy and other Constitutional rights, the City is allowing a private company to create the Privacy Policy that will best reflect its ability to generate revenue from the data it's collecting from the public's mobile and home computing devices. This should have been a non-starter in the first place, but it is clear the City punted on its responsibility to own the creation of the Privacy Policy. **The only thing this can be called is gross negligence on the part of the City, and it must be held accountable for giving away the creation and control of the privacy policy to Alphabet.**

Moreover, the City's Department of Information Technology has decided that it will be the sole reviewer of Alphabet's Privacy Policy. What this means is that the DoIT believes its technology personnel are equipped to make decisions on legal and Constitutional matters as they relate to peoples' privacy and 1st, 4th, 5th, 9th, and 14th Amendment violations by the City. This is not only irresponsible and unprofessional but illegal since they are not professionally qualified to make these policy and legal decisions.

The fact is this: technical personnel are not trained in either the law or public policy regarding privacy, particularly digital privacy. They simply are not equipped with the skill set to make judgments and decisions on matters that affect peoples' privacy and Constitutional rights. Moreover, since the City has a revenue sharing model with Alphabet, it is incited to compromise peoples' privacy and Constitutional rights in order that more device and personal information can be captured by Alphabet so higher revenues can be generated through digital advertising. A privacy policy that is very strict would limit the amount and type of data Alphabet could collect, and control its use. This, of course, would result in lower revenue for itself and the City so neither party would be interested in doing this.

Also, the point needs to be made that the deployment of EBKs is not akin to deploying routers or wireless access points in, say, a campus network used only by employees of the City of New York. In this type of network, the DoIT certainly could take on the responsibility for creating a privacy policy since it applies only to City employees. The EBK network is a completely different ball game, however, for all the issues this document has detailed.

The bottom line is this: the DoIT simply cannot have sole jurisdiction over the Privacy Policy since it does not have the skill set to deal with the serious privacy, Constitutional, and policy issues raised by the EBK network. It is not acceptable for the City simply to review the Privacy Policy created by Alphabet and then give its approval, which is what the process is today. **This is not the right approach to protecting peoples' privacy and Constitutional rights because Alphabet will craft a policy that is in its best financial interests since it uses the device metadata, unique device IDs, user data, personally identifiable data, and other data to generate higher advertising revenue for itself.** And, since the City has a perverse financial incentive to have a weak Privacy Policy

The Stop LinkNYC Primer

due to its percentage-based revenue sharing arrangement with Alphabet, a Privacy Board needs to be created with the aforementioned groups.

The Franchise Agreement’s Privacy Provisions Apply Only to Users, Not Non-Users Who Have Wi-Fi Enabled But Who Do Not Use Any EBK Services.

Alphabet’s Privacy Policy only mentions “users” of its EBK service, and not “non-users” whose MAC Addresses also are captured by the units. As noted in other sections of this document, Alphabet captures unique device IDs (MAC Addresses) when a person has Wi-Fi enabled in their mobile device but is not even a user of EBK Wi-Fi services. By not expressly prohibiting it, the Franchise Agreement allows Alphabet to: 1) use a non-user’s unique device information in any way it likes, and 2) use it to identify a person by cross-referencing it with other databases it owns (or rents or purchases) that may contain both the unique device ID as well as personally identifiable information.

This is a critical point to understand. While it’s bad enough Alphabet can locate and track users of its Wi-Fi services throughout the city at the block and building level 24/7/365, it can also do the same to people who DO NOT use its EBK services (the non-users) but who have their Wi-Fi enabled. Since the vast majority of non-users will have their Wi-Fi-enabled (all mobile devices have their Wi-Fi turned on automatically when they are newly activated), the EBKs will capture their MAC Addresses all the time.

Alphabet’s Privacy Policy Provisions on Disclosing Personally Identifiable Information Violate Section 4.4.4 of the Franchise Agreement

Alphabet's privacy policy violates section 4.4.4 of the Franchise Agreement’s SRV Addendum because it states that it can, and will, disclose personally identifiable information. The Franchise Agreement makes it clear that this cannot be done, even if a user consents to it. There is no provision in the Franchise Agreement that allows a user to consent to having their personally identifiable information sent to anyone outside Alphabet. Franchise Agreement SRV Addendum Section 4.4.4 on Privacy is as follows:

(i) ***Franchisee shall not DISCLOSE Personally Identifiable Information concerning any User*** and shall maintain at all times the best prevailing practices among public Wi-Fi networks (including the cryptographic scrambling of any Personally Identifiable Information and Technical Information that is collected) to safeguard such information against unauthorized access, loss, or unauthorized disclosure to any person other than the User or — to the extent necessary to operate the System — the Franchisee. Notwithstanding the foregoing, Franchisee may disclose Personally Identifiable Information to the extent required by law enforcement as part of a criminal investigation or an investigation related to national security, provided that Franchisee has a good faith belief that such disclosure is reasonably necessary to satisfy law, legal process or enforceable governmental request.

(ii) Additionally, Franchisee may disclose Personally Identifiable Information concerning any User in response to a civil legal demand, unless prohibited by law, and only if Franchisee provides reasonable prior notice to the extent possible to the User and the City before disclosing the information.

(iii) ***The Franchisee will not collect any such Personally Identifiable Information concerning any User except to the extent necessary for TECHNICAL management of the Wi-Fi Service.***

a) “Personally Identifiable Information” means any information which personally identifies the person to whom such information pertains. Personally Identifiable Information includes: name, address, phone number, fax number, email address, financial profiles, biometric information, medical profiles, social security number, and credit card information. Personally Identifiable Information does not include information that is collected or stored in a manner that no longer reflects or references an individually identifiable user ***[Commentary: this latter provision is a major loophole in the definition of “personally identifiable information” since it allows***

The Stop LinkNYC Primer

Alphabet to collect PII for any reason, not just for technical management of the Wi-Fi service. In addition, the City is relying exclusively on Alphabet's good faith it will not store the collected information or data in a way that can personally identify a user. The City has no way to audit whether Alphabet is actually doing this however and it's not in the City's financial interest to do so.]

b) "Technical Information" means Information (which by itself is not Personally Identifiable Information) such as a unique identifier, location information, IP address or MAC address. Technical Information that is associated with Personally Identifiable Information will also be considered Personally Identifiable Information.

Alphabet's privacy policy details how it can and/or will disclose personally identifiable information in the sections, "How Your Information May be Used", and "How We Share Your Information".

It states it will give personally identifiable information to third parties upon consent of a user: **"In addition, with your opt-in or consent we may use your information, including Personally Identifiable Information, to:**

- Provide you with information about goods or services that may interest you;
- Permit selected third parties to provide you with information about goods or services that may interest you;
- Send you emails about updates, information, or alerts regarding the Services."

So, while the Franchise Agreement explicitly states in section 4.4.4 section (iii) that personally identifiable information cannot be collected or disclosed to third-parties, Alphabet crafted, and the City approved, a Privacy Policy that allows it to do just that. In addition, if Alphabet requires users – upon gaining access to its EBK Wi-Fi service - to consent to share their personally identifiable information with parties outside of the company, then that would be a violation of the Franchise Agreement. This would be an illegal tie-in between the use of EBK Wi-Fi services and the consent to provide personally identifiable information to other parties. This would render the Franchise Agreement's section 4.4.4 meaningless.

The City's Financial Agreement with Alphabet Constitutes a Conflict of Interest and is Contrary to Protecting Peoples' Privacy.

The Franchise Agreement's revenue section specifies that the City will share advertising revenue with Alphabet at a level of 50% for seven years and then reap a majority (55%) of advertising revenue starting in year 8 and ending at the termination of the contract. It also receives a 50% share of non-advertising revenue from the company through the life of the contract. By having this type of variable percentage-based revenue sharing arrangement (with a minimum floor of \$500 million over 12 years), the City has incited itself to compromise peoples' privacy and Constitutional rights, the aesthetics of the city, and quality of life of resident and visitors.

The reason this is true, as explained in the beginning of this document, is because Alphabet generates the vast majority of its revenue through digital advertising. The more data Alphabet can collect on people and devices in New York City, the higher the rates it can charge to its advertisers since they will pay higher fees for more granular information about their target audiences. Specifically, the more data points the EBKs capture the greater Alphabet has the ability to target its ads on its EBKs, the websites it owns, and on 3rd-party websites. Alphabet's advertisers are willing to pay more for this type of targeting, which means higher revenue for Alphabet. And, pursuant to the variable revenue sharing agreement as detailed in section 6.3 of the Franchise Agreement, it means higher revenue for the City.

The City understands this aspect of Alphabet's business model very well, and it has teamed up with the company to maximize government revenue by taking advantage of, and abusing, its residents' and visitors' device and personal information. **The City's variable revenue model with Alphabet means that it is incited to allow Alphabet to collect as much data from people and their devices, and thus compromise their privacy and Constitutional rights. Section 6.3 of the Franchise Agreement specifies the variable revenue agreement:**

The Stop LinkNYC Primer

Contract Year	Minimum Annual Guarantee	Percentage of Gross Revenue Advertising	Percentage of Gross Revenue – Non Advertising
Contract Year 1	\$20,000,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 2	\$22,500,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 3	\$25,000,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 4	\$27,500,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 5	\$42,000,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 6	\$47,000,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 7	\$51,500,000	Fifty (50%) Percent	Fifty (50%) Percent
Contract Year 8	\$57,983,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 9	\$59,722,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 10	\$61,514,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 11	\$63,291,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 12	\$65,119,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 13	\$67,001,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 14	\$68,938,000	Fifty-Five (55%) Percent	Fifty (50%) Percent
Contract Year 15	\$70,932,000	Fifty-Five (55%) Percent	Fifty (50%) Percent

When a government decides that money is more important to it than its peoples’ privacy and natural rights, it means they are being “sold out” and treated as subjects, not as free people. This is precisely what the City of New York has done. Importantly, the City has become a “private corporate partner” of Alphabet that is more interested in filling its coffers than it is in being a government “of the people, by the people, and for the people”. This type of business relationship with corporations is a dangerous consequence of “public-private partnerships”, since the government loses its mission to serve and protect people and instead compromises their rights and interests by selling out to for-profit businesses because it can make money. By becoming, essentially, part of the private corporate structure of Alphabet, the City is incited to maximize its revenue at all costs to the public – that is, the cost of violating its residents’ and visitors’ personal privacy and Constitutional rights - as well as the aesthetics of New York City and the quality of life by forcing people to look at electronic advertisements on virtually every block.

While the City may argue that people have a way to opt out of their device or personal information being used against their will by simply turning off Wi-Fi, the fact is that this simply is not realistic. And as we have seen already, Alphabet has – without authorization – turned on Wi-Fi in devices that have it disabled. So even if someone does turn Wi-Fi off, Alphabet can turn it on without a user’s authorization whenever it wants to (see previous section above that addresses this). Both the City and Alphabet know that people don’t turn off Wi-Fi as a regular course of using their devices, or that they may forget to turn Wi-Fi off after using it. In addition, there may be a high percentage of people who don’t even know that their mobile phones have Wi-Fi capability and that it is turned on automatically upon new activation. And, even if someone does know their device has it, they may not 1) know that it is turned on automatically upon new activation, or 2) think about turning it off immediately upon new activation. And most importantly, due to its large market share of mobile operating systems, Alphabet has vast market power with Android, so it can force device manufacturers to configure Wi-Fi to be enabled upon a new activation. So, the City’s business relationship with a dominant market participant in mobile operating software (Alphabet), has turned it into a “willing executioner” of its residents and visitors, since it knows that its business partner has market power to force mobile devices using its operating system to turn on Wi-Fi automatically when new devices are activated.

The Stop LinkNYC Primer

Moreover, public-private partnerships pose an incredible danger to the democratic process because they can allow governments to raise considerable revenue beyond that which is set by its legislative body, which has the power over the purse. This is a core concept of American democracy and if the creation of a public-private partnership circumvents the legislative body's power to raise government funds it is a violation of both the spirit and letter of the separation of powers. While the LinkNYC EBK network may have been approved by the New York City Council – the legislative branch of the City of New York - the operational aspects are left to the Executive branch, which may be able to operate the business unilaterally as a way to massively increase the City's budget. There comes a point at which the Executive branch's ability to raise large amounts of revenue that are not related to costs in any way (such as with fees) is a violation of the separation of powers and the legislature's sole role in raising revenue for the government. It allows the government to expand its budget simply by teaming with corporations, instead of getting consent from the people.

In addition to this threat to democracy, public-private partnerships are also a significant danger to the free, competitive marketplace. In the case of the EBK network, it is a monopoly franchise for Wi-Fi service that no other company can provide. It is in direct competition to other wireless services operating at different parts of the radio spectrum (such as cell service using CDMA), as well as wireline services such as cable-based Internet service. The City has created a situation where it and Alphabet own the monopoly for Wi-Fi service throughout New York City; and, starting in year 8 the City becomes the majority stakeholder in the monopoly since it reaps a majority of its revenue. This could have extremely negative effects on the existing market for wireless and wireline broadband service (see Monopoly and Anti-Competition section for further discussion).

No Mechanism Exists to Count and Audit the Number of Inquiries Alphabet Receives from any Government Entity or Individual

The City has not established a mechanism (or has not published it if it has) to count, track, and disclose the number of times Alphabet receives inquiries from it or other governmental bodies for information on peoples' devices or on the people themselves. The residents and visitors of NYC deserve to know to what extent government is accessing device information, personally identifiable information, and service usage information and for what reasons. Without this type of disclosure, the City and other governmental agencies are incited to make as many inquiries as possible since their requests are shielded from the public, even though it's the public's information it is obtaining and analyzing. Again, as mentioned previously, non-users of EBK services have not even consented to the capture of their data by Alphabet, yet the government can get access to and analyze it.

A Bill of Material (BoM) and a Process for Testing EBKs are Needed in Order to Protect Privacy

From the Beta Test of the EBK network and documentation provided by Alphabet in its Privacy Policy, it has been revealed that the City and Alphabet already have violated the terms of the Franchise Agreement by allowing unauthorized features and capabilities into the units. These include video recording, audio recording, audio sensing, photography, and Web browser software.

Because of both the privacy threats of the EBKs and the need of Alphabet and the City to conform to the legal terms of the contract, the City must ensure there is a process by which to technically evaluate **each** EBK to ensure no additional hardware, firmware, or software are contained in them beyond that allowed by the Franchise Agreement. This process will ensure that only the allowed features and capabilities are part of each unit. **This must be done through a Bill of Material (BoM) provided to the City and independent entities for each EBK, and must include the physical and technical inspection of the units and their hardware, firmware, and software.**

The Stop LinkNYC Primer

A Bill of Material (BoM) for each EBK should be sent to the following entities:

- a) The City of New York (including DoIT, Franchise Concession, the City Attorneys, City Council, Mayor's office, Community Board Leaders, Public Advocate, and others).
- b) Two independent digital privacy organizations.
- c) Two technical laboratories chosen by the two privacy organizations.

Each of these entities needs to evaluate the BoM from their respective positions and charters. The technical laboratories can have no prior or future business relationship with either Alphabet or the City. It is critical to have multiple digital privacy organizations and technical labs involved in this process for the following reasons:

- a) To generate discussion and ideas on the Bill of Material.
- b) To serve as a check and balance on the City and Alphabet.
- c) To mitigate the potential of Alphabet and the City exhibiting undue influence or bias on the Bill of Material evaluation process

The BoMs must come directly from the manufacturer of the EBKs in hard copy and digital formats, and not from Alphabet. If Alphabet does the entire assembly of the EBKs, then personnel from an independent technical lab should be brought in during assembly of **each** EBK in order to visually and technically examine each unit to ensure compliance with the contract. Otherwise, Alphabet could include unauthorized capabilities and falsify the BoM that it gives to the City and independent entities.

3) For EBKs already installed, their hardware, software, and firmware needs to be inspected. This technical work needs to be done by the City and the two independent technical labs chosen by the digital privacy organizations. This must include physical inspection of each unit on-site at each installation.

The City also needs to ensure that Alphabet is not able to make unilateral software, firmware, or hardware updates or upgrades to the EBKs without first going through an official public evaluation process that details everything about the changes. This includes any update or upgrade that is related to a security or performance issue, or desired goal. Any updates or upgrades for any hardware, software, firmware, or other components need to include an evaluation by the independent digital privacy and technical organizations to ensure they do not violate personal privacy and rights.

Without a Bill of Material that is Verified by an Independent Board, Alphabet Could Include Non-Authorized Capabilities to Locate and Track People, Among Other Things

By not having a rigorous Bill of Material process, Alphabet could integrate capabilities and features into the EBKs, particularly those that violate privacy such as technologies related to locating and tracking people. For example, Alphabet could integrate cell phone wireless capability, which operates at a different radio frequency from Wi-Fi. The reason Alphabet might want to include cell phone capability is to pick up a unique device ID (MAC Address) when a cell phone's Wi-Fi has been turned off. It is rare that someone turns off their cell service by invoking airplane mode or shutting down their device, so for those who don't have Wi-Fi turned on Alphabet could capture MAC Addresses transmitted via cell phone radio frequencies (such as CDMA). Once it has the unique device ID, Alphabet could locate, track and possibly display advertising to the device when it's being used to surf the Web.

A product popularly known as Stingray is used by various law enforcement entities to capture cell phone metadata and content (conversations, texts, etc). This type of product mimics a cell phone antenna tower by tricking a cell phone into connecting to it. This technology is used by law enforcement agencies in criminal investigation efforts. It is a controversial product because it captures everyone's cell phone information in the area it's being used, not just that of a person under official investigation. Because of this, it raises 1st, 4th, 5th, 9th, and 14th Amendment issues for everyone not under investigation.

The Stop LinkNYC Primer

It's possible that Alphabet may want to install Stingray-type technology in the EBKs in order to capture the unique device IDs (MAC Addresses) being transmitted by people who don't have Wi-Fi enabled in their mobile devices. While the EBKs may not provide the actual underlying cell phone end-to-end communications service that a Stingray-type device might be able to, Alphabet wouldn't care. All Alphabet would care about is the unique cell phone ID and other device metadata it can capture so it can locate and track devices and people. It could then cross-reference this data with other data it has on the device or with personally identifiable information. For example, if the person uses any of Alphabet's other services (such as Google Search, Gmail, or other Google services where users open an account with personally identifiable information), Alphabet could identify the person via cross-referencing the unique device ID it captured via its Stingray-type technology with the personal account information it has in another database that also contains the device's unique ID (obtained by reading the MAC Address in an IPv6 IP Address).

Disturbingly, the Franchise Agreement allows Alphabet to include technology utilizing parts of the radio spectrum not reserved for Wi-Fi. Section 4.1.5 of the Franchise Agreements SRV Attachment states the following:

*"Wi-Fi Service(s)" means the provision of continuous, uninterrupted, unrestricted, free Wi-Fi (wireless fidelity) service, **or similar wireless service of comparable use approved by the City**, to Users of the internet on Wi-Fi enabled devices.*

What the City has done in the Franchise Agreement is to expand the type of wireless service Alphabet can provide beyond Wi-Fi service operating at the 2.4Ghz and 5GHz sections of the radio spectrum. This means that it could legally integrate Stingray-type of technology that operates at the radio frequencies reserved for cell phone service providers, or the cellular technology, such as CDMA, that wireless carriers use for their service.

It bears repeating: the vast majority of Alphabet's revenue is derived from digital advertising. Since some people don't use Wi-Fi, it would be financially beneficial to Alphabet – and the City - to be able to track unique device IDs (MAC Addresses) via the cell service radio frequency (such as CDMA) since it may be able to provide wider advertising opportunities to its advertisers, among other thing.

Storage and Access to Cell Phone Metadata and Content, and Website URLs and Content

Alphabet will be collecting and storing vast amounts of data, including cell phone metadata, Web browsing metadata and content, video, location data, photographic images, street audio, and peoples' conversations. The volume of information it will collect – perhaps trillions of data points each year on millions of people and their devices - raises critical questions that need to be addressed. Below are questions that need to be discussed and answered:

- 1) Do people want their location and other information captured and stored either by a private entity (Alphabet) or the government (the City of New York)?
- 2) Do people want a private company having granular location and tracking information – down to the block and building, 24/7/365 - on millions of devices and people?
- 3) Do people want a company they don't do business with to track their location via their mobile device unique ID (MAC Address)?
- 4) Do people want a private company and/or the City to video record and/or audio record them?
- 5) What type of data is stored on them and their devices?
- 6) How much of data is stored?
- 7) How long is data stored for?
- 8) Is the data erased when it is no longer needed?
- 9) How is the data erased? (Simple deletion or shredded?)
- 10) Is the data stored in EBKs or at a datacenter?
- 11) Is the data stored at an Alphabet or NYC datacenter?
- 12) Is the data stored at a third-party Cloud provider's datacenter?

The Stop LinkNYC Primer

- 13) Is the third-party Cloud storage provider a reputable company with high physical and digital security?
- 14) What are the physical and digital security aspects of the stored data?
- 15) Who has access to the storage devices?
- 16) Is there a record kept of when the storage devices are physically and digitally accessed and who and what titles are allowed to access them?
- 17) Are non-employees, such as contractors and partners, allowed access to the data?
- 18) Does the public have the right to access the stored data?
- 19) What data does the contract allow NYC to obtain from Alphabet?
- 20) What is the City's definition of aggregate data?
- 21) What is the City's definition of anonymous data?
- 22) What is the City's definition of aggregate anonymous data?
- 23) What does the City mean in the Franchise Agreement section 4.4.4, subsection iiiia , that Personally Identifiable Information can be stored by Alphabet as long as it's no longer personally identifiable?
- 24) Is Alphabet or NYC allowed to do analytics on the stored data?
- 25) What type of analytics can be done?
- 26) Can Cookies or other computer software such as Beacons be used to ascertain personally identifiable information?
- 27) If one logs into and uses an EBK with a mobile device and then uses their home Wi-Fi, will Alphabet be able to use an EBK Cookie or Beacon in its advertising to associate home Web surfing with the person's use of the EBKs or their geo-location?
- 28) Are Alphabet and the City allowed to cross-reference unique device IDs with other databases that contain both it and personally identifiable information associated with it?
- 29) If Alphabet claims neither device-specific nor personally identifiable analytics are being done, how can the City technically audit and verify this? If the City claims the same, how is the City audited?
- 30) If the contract between NYC and Alphabet does not allow the public or other companies access to all stored data, what is the reason for this? Is it to provide Alphabet with sole ownership of the public data so that the company can generate revenue from it while others can't?
- 31) Does an individual have the right to know what data has been stored for their device?
- 32) Is there a mechanism or process by which a person can demand that none of their device's data be stored?
- 33) Are Alphabet or NYC using third-party companies in their analytic efforts? (which would mean a person's data is being sent to another company, which would be a violation of the Franchise Agreement).
- 34) Are real-time analytics being done – either known or unknown to a person - that can deliver advertisements on-the-fly? For example, an individual walks down the street and through real-time analytics Alphabet can send advertisements to the device for stores that are located in the direction the person is walking.
- 35) Are Alphabet or NYC analyzing the data to reveal the identity of the person who owns the mobile phone?
- 36) Is Alphabet generating revenue from the stored and/or analyzed data, outside of the fees it charges to advertisers? If so, how much is it making?
- 37) Can EBKs support software-based Stingray-type technology?
- 38) Can EBKs support radio frequencies reserved for cell phone wireless service through either hardware or software? Can they support Bluetooth frequencies?
- 39) Can EBKs support Automatic License Plate Reader technology?

The Beta Test

Beta Test Criteria and Time Period

Alphabet and NYC embarked on a beta test of the EBKs in the first half of 2016. There is no easily accessible information available to the public on the following:

- 1) The beta test criteria and goals for both Alphabet and NYC.
- 2) How the beta test criteria and goals were developed/derived by both entities.
- 3) The success metrics established by both Alphabet and NYC.
- 4) How the success metrics were developed/derived/chosen by both entities.
- 5) How NYC will be able to evaluate the beta test goals and metrics it established for success or failure.
- 6) How NYC will be able to audit the beta test outcomes and results presented by Alphabet to ensure the company is not falsifying the data in order to show high usage of the EBKs when in fact it is low.
- 7) The length of time for the beta test.

Some examples of criteria that the City (not Alphabet) should cover in its portion of the beta test are listed below. Results for many of these should be published on a weekly basis; other results should be published bi-monthly and still others at a reasonable time so that the public has time to evaluate the data and provide feedback.

- 1) The absolute number and percentage of the “over 25% of New Yorkers who lack high-speed broadband service who have used the EBKs, including where and the number of times each has used them. Alphabet and the City claim, without any independent statistically significant research, that this percentage of people lacks high-speed broadband service, which implies they want it but can’t afford it – but it’s not really clear what this number represents. Voice and text can’t be included in this claim because people can get free cell phones from the federal government if they qualify.
- 2) What percent of the “over 25%” is accessing the EBKs through handheld devices? Through home computers?
- 3) What the services were used for (e.g., emergency calls, calls to friends and families, watching music videos, watching pornography, watching Youtube and similar services, making international making US long distance calls, making local calls, powering up devices, etc.).
- 4) The percentage of people residing in the U.S. illegally using the services, and which services they use.
- 5) The length of time each of these people used a service.
- 6) The number of services and which ones were used.
- 7) The overall value of the services and peoples’ satisfaction level with Quality of Service (QoS).
- 8) Whether people believe free wireless broadband is worth having 10,000 EBKs with electronic, rotating ads deployed on virtually every block of the city.
- 9) Whether people like or dislike the physical size and shape of the EBKs.
- 10) What they feel about the aesthetics of having the large Wi-Fi units on virtually every block of New York and whether they feel the modern design is consistent with their neighborhoods.
- 11) Whether people like or dislike having electronic ads in their residential neighborhoods.
- 12) To what extent people are distracted by the electronic ad rotation scheme.
- 13) To what extent do people like or dislike partial or full motion video ads.
- 14) To what extent people are physically and mentally annoyed and/or harmed by their eyes and head being forced to turn and look at the electronic ads because of the rotation scheme, size of the units, bright colors, and complex ad designs.
- 15) What people think about the advertisements’ wide range of colors and complex shapes and graphics.
- 16) To what extent users and non-users are concerned about their privacy (this would require the City to explain the ways that Alphabet and the City can use and analyze the metadata, location data, and personally identifiable data that the EBKs collect).

The Stop LinkNYC Primer

- 17) Whether people think their Constitutional rights are violated by the City being able to track them through their mobile devices.
- 18) Whether the EBKs are capturing non-user MAC Addresses.
- 19) Whether Alphabet is copying and sending all device data captured by its EBKs to remote database servers.
- 20) Whether people know they are being tracked whenever they have their Wi-Fi and/or Bluetooth enabled.
- 21) To what extent people want their whereabouts known down to the block or building, 24/7/365.
- 22) To what extent do motorists and bicyclists want to be tracked by the EBKs.
- 23) To what extent people want recordings made of them through the video, audio, and photographic capabilities of the EBK Wi-Fi units (again, these are illegal capabilities contained in the units).
- 24) What the clarity is of video and photographic recordings.
- 25) Whether cameras are able see inside apartments (including wide and zoom positions).
- 26) Whether the cameras have infrared capability to see and record at night?
- 27) If cameras can be moved by Alphabet, can they be directed at apartments? If so, can they see inside?
- 28) Is there an audio recording capability? Is it able to pick up conversations?
- 29) Is pornography being accessed?
- 30) Are websites that the City does not want or allow access to being accessed?
- 31) Is access to non-allowed websites being done using the EBK screen or through the mobile device screen.

These are just SOME of the beta test criteria that the City should be measuring and evaluating...there are many others. It is only through this type of beta test plan that the City and the public can make an informed decision on whether to continue deployment of the EBKs or have them removed.

Who Should be Involved in Creating the City's Beta Test Plan

The EBKs create new and fundamental privacy, environmental, aesthetic, physical health, mental health, and Constitutional issues that need to be addressed by the public. The City's Department of Information Technology is not equipped with the skill set to create a comprehensive beta test plan, since its employees have only technical backgrounds and simply cannot address all of these non-technical issues. The entities that should be part of the City's beta test plan development include the following:

- 1) Digital privacy rights organizations
- 2) Civil rights organizations
- 3) Government watchdog groups
- 4) Motorist associations
- 5) Border control groups (to ensure illegal immigrants are not included in the beta test)
- 6) Independent technical labs
- 7) City of New York Departments: DoIT, DOT, Community Boards, Public Advocate, Corporation Counsel
- 8) New York State Departments: DoIT, DOT, Attorney General's Office

Without a comprehensive beta test development process for the City, the only beta test that is being conducted is by Alphabet to check the technical and operational performance of the EBK network. Having non-governmental entities be part of the beta test plan development is the only way the public can evaluate and provide oversight to the EBK network business that both Alphabet and the City clearly want to deem successful. **If no City-oriented beta test criteria, best test goals, and beta test success metrics were created before deployment of the EBKs in 2016, that would be grossly negligent conduct – and perhaps illegal. It would raise serious questions as to the competency of those individuals within the City who administered and were involved with this project, as well as their motives. At minimum, it would show a complete lack of understanding of what a beta test is and why it is done.**

The beta test information described above should have been part of the public hearing process. If the City did not have a beta test plan in place (or in development) at that time, one should have been developed and reviewed by various technical and non-technical parties, and finalized **before** the first EBK was deployed. If no beta test plan

The Stop LinkNYC Primer

were finalized before the first deployment, then there is in fact no beta test being conducted by the City. The same holds true for Alphabet – if it did not submit its own beta test plan to the City before the first EBK was deployed then there is no bona fide beta test being conducted.

If beta test plans were created after the first EBK was installed then this would indicate they were created with bias. Beta test criteria established after the Wi-Fi network was operational and being used indicates that both Alphabet and the City wanted to create a test plan based on the actual use of the Wi-Fi network, and work backwards from this data to set the beta test criteria. The reason they would want to do this is so they could prove success of the Wi-Fi network: if usage and operational metrics exceed the beta test criteria - which were established after the deployment of the network - then the City could announce to the public that it was a success.

Auditing the Beta Test

An auditing process needs to be established to evaluate the beta test, both for the City and for Alphabet. This process needs to be run by the City and an outside independent testing lab chosen by a non-profit digital privacy organization that has experience or expertise in usability testing, alpha testing, and beta testing.

The reason to do the audit is to ensure that neither Alphabet nor the City rig the methodology or falsify the results of the beta test, and that the features and capabilities have gone through proper internal testing before deployment. The reason for using an independent outside testing lab is to ensure that the City does not aid or abet the falsification of the data, or at minimum, fails to provide the proper oversight and auditing of the beta test because of its intrinsic bias to have the EBK network deployed (for both financial, surveillance, public policy reasons). The testing lab can also ensure that Alphabet does not include features and capabilities into the EBKs that are not allowed by the Franchise Agreement.

The Ultimate Success Criterion for the City's Beta Test

While there are many beta test criteria to test and measure, the primary criterion for the City is to assess whether the “over 25% of New Yorkers who lack high-speed broadband service” are using the EBK network. Again, as previously discussed, it is assumed Alphabet and the City mean that this population wants broadband service (non-voice service) but either can't afford it or get technical access to it. Many of these people already qualify for free cell phones and free cell service under federal law, so voice and text can't be part of the beta test criteria.

What needs to be measured is whether the “over 25%” population is using the EBKs for non-voice/non-text Internet service. This is the most important criterion to measure because the City has justified the deployment of 10,000 gigantic Electronic Billboard Kiosks in order to serve free broadband service to this population for the purpose of “closing the digital divide”. If the vast majority (90%) of this population is not using the EBKs for non-voice/non-text Internet service then the beta test should be deemed a failure and all units removed. The reader will be reminded that 52% of the required 7,500 units will be deployed in the wealthiest borough of Manhattan, which comprises only 17% of New York City's population. Even with the deployment of the additional 2,500 units in the other four boroughs, Manhattan will still have 39% of the units. Given these deployment percentages, it will be extremely difficult – essentially impossible - for the City to prove that 90% of the “over 25%” are using the free Wi-Fi service.

One of the ways the City may rig or falsify an audit is by not identifying who is using the EBK network; that is to say, it may just count connections to the network and not identify whether those connections are being made by NYC legal residents, NYC illegal residents, or non-residents (commuters, tourists, business visitors, etc). Since the city has so many commuters and visitors, it could be that a significant portion of EBK usage comes from non-residents. Non-resident access to free public Wi-Fi was not included as a reason by the City (or Alphabet) for a) wanting and b) approving the network. Since non-resident usage was not a reason for approving the franchise business, usage of the EBK network by these people cannot be included in an audit or feedback analysis/survey of the system. The City must ascertain which connections are coming from residents – in particular, from the “over

The Stop LinkNYC Primer

25%” population that “lacks high-speed broadband service” – and include only those in its analysis. It cannot include people living in the city or country illegally. This analysis can’t be done by looking at EBK software log files since they do not capture any information that would tell whether a connection was made by a resident of New York City. To execute the feedback for this beta test criterion, the City must conduct a randomized, statistically significant survey of the “over 25%” of the population that lacks broadband service. This means the City must do a number of things:

- 1) Define what it means when it says over 25% of New Yorkers lack high-speed broadband access”.
- 2) Show that “New Yorkers” means people living in the five boroughs of New York City and not the entire state of New York.
- 3) Screen people to ensure they fall under the definition, and exclude from the survey people who can afford high-speed broadband and have technical access to it but don’t want it.
- 4) Exclude from the survey people living illegally in the country.
- 5) Ask survey respondents questions about their access to, desire for, and use of only high-speed broadband services (not voice service since this is not defined as a broadband service...it is a telephone service that can be obtained for free from the government). This means the use of services that require high-bandwidth such as video, file downloads of a minimum size, and other transmissions that include industry-accepted definitions for “large file size” or “high bandwidth”. Web pages without video, email messages, and other services – for example, streaming an MP3 audio file – which don’t fall under either of these two requirements cannot be included in the survey.

The City must pay an independent company to administer the market research, and independent digital privacy organizations and government watchdog groups must be integral to the process in order to act as a check and balance to ensure the City does not interfere with the data collection methodology and the results. These independent bodies need to lead the creation and execution of the survey, with the City providing input as needed and to serve as a resource. The independent bodies need to ensure that the population they are surveying is an accurate representation of the “over 25%” who lack broadband service, and that it does not include illegal immigrants.

Health Issues

Because EBKs are Wi-Fi hotspots, they emit radio frequency (RF) energy that comes into contact with people. Frequent exposure to high levels of RF can be harmful to people. The Wi-Fi hardware equipment being used in the EBKs is “industrial strength” since they can handle 256 connections (compared with home routers that typical have no more than 4 connections). People are being bombarded with EBK Wi-Fi radio frequencies when they stand next to them waiting to cross a street, as well as when they walk down the street. There needs to be proof that the amount of RF to which adults, children, and babies are being exposed - on virtually every block they walk - is not harmful.

This is probably the first time in history that industrial strength Wi-Fi hardware has been located so close to human beings in so many geographic locations. This is particularly true for workers in commercial establishments who businesses are situated directly across or near the EBKs. They are exposed to EBK RF radiation on a continuous basis, perhaps as long as 12 to 16 hours every day. It is not enough for Alphabet and the City to maintain that the Wi-Fi hardware is FCC compliant - they must prove that it is compliant for this particular application where EBKs are located on sidewalks and people will be passing by and standing next to perhaps hundreds of them every day throughout the year. Typically, industrial strength Wi-Fi hardware would be located far away from people, such as in an off-traffic area in an airport terminal or in ceilings, for example. But in New York City they are located a matter of inches away from people. And since there are so many of them, the amount of RF to which people are being exposed is high and constant.

Alphabet and NYC must make information publicly available on the RF energy emitted by the EBKs. They need to show that the equipment used in the EBKs is safe for humans – especially babies, toddlers, and employees of businesses - at distances from zero to 400 feet (the radius reach of the EBK Wi-Fi signal). They need to show that repeated and/or prolonged exposure on a daily basis to hundreds of EBKs is not harmful. They also need to provide, on a regular basis, test results that show the level of RF for each unit. Finally, they need to document and prove that the RF emitted is within acceptable ranges for human of all ages in terms of strength, frequency of exposure, and length of time of exposure.

See Negative Quality of Life Issues Section for additional discussion on occupational safety and health issues, as well as health issues related to the physical and mental well-being of residents of New York City.

Transportation Issues

While the Franchise Agreement makes no mention of EBKs being used for any transportation related activities, this section is included because EBKs could be used for traffic or other transportation reasons given that the Alphabet subsidiary that operates the EBKs, Sidewalk/Intersection, is also involved with transportation solutions through its Sidewalk/Focus entity. Sidewalk/Focus has a business mission of helping to make cities “smart” when it comes to transportation, and Alphabet could violate the Franchise Agreement by co-mingling its EBK franchise – granted only to provide Wi-Fi service and display digital advertisements - for use in its Sidewalk/Focus activities.

By way of some background information, the Federal Department of Transportation granted \$40 million in funds to seven cities for its “Smart Cities” initiative and Sidewalk/Focus is working with them to develop new technologies for transportation infrastructure. While New York City did not receive any grants from the Federal DOT under this program, there is no reason to think that the City will not want to make its streets “smart”.

Since Sidewalk is involved with the Smart Cities initiative, there are a number of potential ways it (and the City) could leverage the EBKs in ways not authorized by the Franchise Agreement, including:

- 1) Using unique device IDs from motorists’ Wi-Fi enabled devices or Wi-Fi enabled vehicles to collect data on traffic flows.
- 2) Using video and audio to monitor and record traffic.
- 3) Using video to track individual vehicles.
- 4) Using video or photographs to read vehicle license plates.
- 5) Using the electronic billboards to display messages to motorists.
- 6) Using the electronic billboards as street signs.

Collecting Data on Traffic Flows Using Unique Device IDs from Motorists’/Passengers’ Wi-Fi Enabled Devices or from Wi-Fi Enabled Vehicles

The City may want to use the EBK network to capture the unique device IDs from motorists’/passengers’ Wi-Fi enabled devices or from Wi-Fi enabled vehicles in order to track traffic patterns for transportation planning and operational purposes. As this document has already outlined, there are major privacy and Constitutional issues associated with tracking people, motorists, passengers, and vehicles via unique device IDs from mobile devices or from on-board vehicle Wi-Fi.

And, as this document has explained in previous sections, Alphabet could easily use “anonymous” unique device IDs (MAC Addresses) captured by its EBKs to derive personally identifiable information due to the company’s larger business model. If its transportation subsidiary Sidewalk/Focus were to use the EBKs to track traffic flows, it would be tracking all motorists in New York City, and could personally identify many or all of them. The way it could track them would be by running analytic software programs to identify drivers and passengers in cars via the timing of their devices or vehicles (both being Wi-Fi enabled) passing by EBKs while driving in the city. The way it could personally identify them is by running an analytic software program that cross-references the database containing unique device or vehicle IDs its EBKs captured (the MAC Addresses) with other databases it owns (or rents from 3rd parties) that contain both the unique ID and personally identifiable information. The same tracking, privacy, and surveillance issues that already have been addressed with pedestrians and their Wi-Fi enabled devices apply equally to motorists (and bicyclists).

In addition, there is an effort on the part of the Federal government to mandate that all vehicles communicate with one another via wireless technology. If this technology is adopted, it could be the case that vehicle VIN numbers, plate numbers, and other unique identifiers or personally identifiable information could be broadcast by a vehicle to Wi-Fi access points, like the EBKs. If this were the case, then EBKs could capture all of this information, which could be used to personally identify a driver.

The Stop LinkNYC Primer

Whatever the transportation planning and operations issues are with traffic flows in New York City, they need to be researched without tracking motorists and passengers through their Wi-Fi enabled devices and Wi-Fi enabled vehicles, anonymously or otherwise. There is absolutely no justification for the City to invade motorists' and passengers' privacy in order to resolve either short or long-term traffic issues.

The NYC DOT needs to use internal employees or contract personnel to physically go to problem areas and observe and record what the traffic issues are; it simply cannot use non-consenting and unaware motorists' and passengers' unique device and vehicle IDs (MAC Addresses) to be data points for their transportation research.

EBKs Might Contain Technologies to Read and Record License Plates, Which Would Allow the City to Locate and Track Vehicles Down to the Block, Building, and Garage.

Because the City has already violated the Franchise Agreement by allowing unauthorized non-communications capabilities to be part of the EBKs (audio, audio sensing, video, and image monitoring and recording), it also might want to include other unauthorized capabilities, such as those that can read and record license plates. It potentially could do this through two methods: 1) using a combination of photographing license plates with the EBK video cameras and using off-line image recognition software to identify the vehicle owner, and 2) Automated License Plate Reading (ALPR) technology. ALPR is used increasingly by law enforcement on police cars as well as by transportation departments for tolling, surveillance, and other purposes. The City might want to integrate ALPR into the EBKs so it can track vehicles throughout the City, 24/7/365.

There is No Justification to Use EBK Video and Audio to Monitor and Record Traffic

There is nothing that EBK video or audio sensing or recording can do that traditional traffic cameras can't do when it comes to monitoring traffic. The EBK video does not have a value-add over traffic cameras and there's nothing material that audio sensing could add to traffic analysis. The City simply does not need to video monitor or record **every block** of New York for traffic purpose...this would just be a solution looking for a problem. Moreover, using EBK video and audio for traffic monitoring is not as efficient as using strategically placed traffic cameras situated at higher distances from the ground (than the EBK cameras) since they have both a longer and better field of view. And importantly, traffic cameras can be pointed only at the street, whereas EBK cameras see into peoples' homes and commercial businesses.

Finally, cameras are not needed for assessing major traffic issues. Any major traffic issue must be evaluated by DOT personnel who go onsite to the problem location and do the research. Once a traffic issue is resolved there is no further reason to monitor the location. Having fixed cameras on EBKs at every intersection does not make operational sense at all for long-term traffic issue resolution or mitigation.

Using EBK Electronic Displays to Message Motorists is Not Essential

The City may want to engage motorists with various types of messages relating to driving, traffic, road conditions, construction, and other things. **None of these reasons are important enough to justify the deployment of 10,000 EBKs.** Any type of temporary message (for construction work, for example) can be done through the traditional temporary electronic traffic signs. These types of signs are displayed until construction is done and then taken down. As is commonly believed among motorists, the messages displayed about traffic problems on electronic signs deployed on the country's major highways and parkways are not helpful. In many cases they are unproductive since they cause unnecessary traffic slow-downs that results in more pollution and longer travel times. The fact is, seeing a message that there's a traffic jam for the next six exits doesn't get a motorist anywhere any faster, and it is not often that people take alternative routes, especially if they are not familiar with an area. The country has had electronic signs on its highways for years now and they have not helped alleviate traffic or congestion one bit...everyone can now agree on this fact. In addition, the City's desire to message motorists about traffic laws, buckling up, driving safely, etc. are not important enough to warrant the deployment of 10,000 EBKs. Finally, the City should not be trying to get drivers in New York City to look over to the side of the road to read messages when they are essentially engaged in a near demolition derby when the lights turn green.

Issue Regarding Government Using EBKs to Display Traffic Signs and Messages

When first deployed in the first half of 2016, EBKs displayed public service messages to motorists. This raises questions:

- 1) Who is authorized to create messages for drivers?
- 2) What are the topics that are to be covered by the messages?
- 3) Does the content conform to Federal and State DOT laws and regulations?
- 4) Who is involved in creating these messages? Alphabet, Alphabet's marketing vendors, NYC, NYC DOT, NY State DOT, Federal DOT, etc?
- 5) Do the physical size of a message, the font size, font color, background color, and the physical size of the EBK-functioning-as-a-road-sign conform to Federal and State laws and regulations on traffic signs?
- 6) Does the spacing of the EBKs-functioning-as-a-road-sign conform to Federal and State laws? (The EBKs will be deployed on virtually every block of New York City).
- 7) Do drivers really need to see the same message on virtually every block they drive down? For example: are drivers expected to see a message that says "Buckle up, it's the law" on each and every EBK as they drive, say, on 3rd Avenue from West 14th Street to West 96th Street? There are 82 blocks between these locations and if EBKs are located on every other block a driver could see the message 42 times. When does this type of messaging turn into a form of government harassment? When does this type of thing turn into just complete nonsense and idiocy?

Monopoly and Anti-Competition Issues

Alphabet's EBK monopoly franchise poses a potentially serious threat to the free market for existing wireless cell service providers (such as Verizon Wireless, ATT Wireless, T-Mobile) as well as to wireline service providers such as Cable and Telephone companies (for example, Verizon FiOS and Comcast/Spectrum).

The 10,000 EBKs Could Cannibalize High Amounts of Revenue From Existing Wireless and Wireline Broadband Providers

The large number of EBKs and their collective broadband connections could be a significant competitive threat to the business models of wireless and wireline broadband companies. The Franchise Agreement requires Alphabet to deploy 7,500 EBKs, with an option of up to 10,000. Each EBK is required to support 256 broadband connections with a combined throughput of 1 gigabyte, or about 40 megabytes per connection. This means that the EBK network as a whole should be able to support two million five hundred and sixty thousand (2,560,000) simultaneous connections – 10,000 EBK nodes times 256 connections per node. Since the EBK network connections are not dedicated to any particular user (that is to say, they are shared connections), the 256 access points per unit will handle well more than that number of people. So, the 2,560,000 connections is the minimum number of people who could be served by the 10,000 EBKs; it is likely that the EBKs could service every single one of the 8.5 million people living in New York City, assuming each connection supports 4 individuals (4 people times 2.56 million connections equals over 10 million people).

Since an EBK's signal can reach a vertical height of 150 feet (and possibly 400 feet) in both horizontal and vertical directions, it means the network will be accessible to any residential and commercial units located up to the height of a 20 story building (assuming 8 feet per story and a maximum Wi-Fi range of 150 feet). Since New York City has around 3.3 million housing units, if it's assumed that 90% of NYC housing stock is located within 20 stories from the ground, it means the EBKs could reach about 3 million residences (adding commercial businesses into the equation increases the number). If the maximum Wi-Fi range of an EBK is 400 feet, then that would mean it could reach units as high as 50 stories, increasing Alphabet's total available market to perhaps 99% of the city's population.

The EBK Network Provides a Large Percentage of Residents the Option to Cancel Their Wireless and Wireline Fee-For-Service Internet and Cable Service

Since the EBKs provide free broadband Wi-Fi service, it could mean that a large number of households might cancel both their fee-based Internet broadband service and their Cable TV service, or at minimum just the Internet service. Alphabet's marketing material shows that it is seeking to serve more than the "over 25%" population it (and the City) claims "lack" broadband service:

*"Over 25% of New Yorkers lack high-speed broadband at home. LinkNYC [the EBKs] will address this glaring digital inequality by making the fastest public Wi-Fi in the world freely available to millions of people for the first time. **Many more will be able to reduce their spending on data plans.**"*

If a large number of consumers served by the existing fee-for-service wireless and wireline broadband providers cancel their service subscriptions, it could be a material competitive threat to companies such as Verizon Wireless, Verizon FioS, Comcast/Spectrum, ATT Wireless, T-Mobile, Sprint, Virgin, and many others. The Franchise Agreement calls for Alphabet to provide state-of-the-art technology, which means that it could provide ever-increasing throughput speeds. This would mean a greater competitive threat to fee-based service providers for Internet and Cable service (Cable is included because an increasing number of people are "cutting the cord" or "cord nevers" and receive television and movie programming through their broadband Internet service). The same is true for wireless cell service providers, where their customers could cancel their service and use the EBK Wi-Fi network for all their television, movie, gaming, and other video needs.

The 10,000 EBKs Could Negatively Effect the Market Value of Publicly-Held Wireless and Wireline Broadband Providers

In April 2017, Verizon released its Q1/2017 earnings report and announced that it had lost 307,000 wireless subscribers. In Q1/2016, Verizon had a gain of 640,000 wireless subscribers. Total revenue for the company in Q1/2017 declined significantly by 7%. A material part of this huge reversal in subscribers and revenue may have come as a result of the free EBK Wi-Fi network in New York City. Because of the competitive threat free EBK Wi-Fi service poses to fee-based broadband wireless and wireline service providers, those companies that are publicly held have a fiduciary obligation and a duty of care and loyalty to reveal this situation to its stockholders. If the competitive threat of EBK Wi-Fi service is material to their businesses, these companies are required by law to conduct financial analyses on how the potential loss of customers could impact their revenue streams. The services they need to consider in their analyses include Internet, telephone, Cable Television, On Demand, streaming video, streaming audio, DVR services, and fees associated with hardware and software related to those services that would be lost if customers cancel services. Below is a very simple example of what this type of analysis might look like:

Number of Households Canceling Service	Potential Average Monthly Revenue Loss per Household**	Potential Total Revenue Loss to Industry in New York City per Month***	Potential Total Revenue Loss to industry in New York City per Year
2,500,000*	\$50/mo	\$125 Million	\$1.5 Billion
2,500,000*	\$55/mo	\$138 Million	\$1.7 Billion
2,500,000*	\$60/mo	\$150 Million	\$1.8 Billion
2,500,000*	\$65/mo	\$163 Million	\$2.0 Billion
2,500,000*	\$70/mo	\$175 Million	\$2.1 Billion
2,500,000*	\$75/mo	\$188 Million	\$2.3 Billion

*While it has not provided any independent, 3rd-party data to support their claims, Alphabet and the City assert that “over 25% of New Yorkers lack high-speed broadband service”, which is assumed to mean that a) they live in the five boroughs of New York City and does not include others living in the state of New York, and b) these people want it but can’t afford it or get technical access to it. It is also assumed that these people are living in the country legally. Accordingly, the 2.5 million households reflects 75% of the 3.0 million housing units (reachable by the EBKs at a Wi-Fi range of 150 feet) that already have broadband service and/or Internet service either through mobile devices or home routers and cable boxes. It is this population from which the EBKs could siphon off users of broadband and/or Internet service from wireless and wireline companies. If the EBK Wi-Fi range is 400 feet, then the number of households to include in the analysis would be almost all residences, or 3.3 million.

**the average price per month a household pays for broadband cable, Internet access, or both. This is the amount households would not have to spend per month with fee-based wireline and wireless broadband and Internet service providers if they used free and/or fee-for-service EBK Wi-Fi services. This includes mobile phone service, home Internet, home telephone, and cable television, as well as other services and fees associated with On Demand, DVR, and hardware rental fees.

*** Reflects the average monthly revenue loss to existing providers of wireline and/or wireless broadband and/or Internet service.

The Stop LinkNYC Primer

The example above is **not** provided to show what the revenue loss **will be** to existing wireless and wireline broadband and Internet carriers. There are many other factors and assumptions that need to be taken into account in order to do a rigorous financial analysis. The simple analysis presented here is to illustrate the type of approach publicly held companies, existing and potential stockholders, and capital market analysts need to take in order to assess the potential negative revenue effect that free EBK Wi-Fi broadband service could have for existing market participants in New York City. The analysis, of course, would need to include the net present value of future revenue streams. If the amount of ongoing revenue loss would be material to the income statements of publicly held companies, they would likely need to disclose this in SEC filings. Additionally, since Alphabet is presumably looking to replicate its free wireless broadband EBK service in other American cities, these companies also likely would have to disclose the potential negative revenue effect for those geographic locations.

Alphabet and the City May Have Created Their Public-Private Monopoly Partnership in Order to Destroy the Competitive Marketplace for Wireless and Wireline Internet and Broadband Services so They Can Reap the Financial Benefits for Themselves

Because of the Franchise Agreement's variable revenue sharing model, the City could reap large financial rewards from the EBK Wi-Fi network. In Year 8 of the contract, it will become the majority revenue owner of the public-private business partnership, receiving 55% of advertising revenue and 50% of fee-for-service revenue. And in addition to the fee-for-service revenue, the City will also collect taxes on those services. The importance of this percentage-based revenue sharing model cannot be overstated: it is a primary driver for the City and Alphabet to not only compromise peoples' privacy but also to destroy the competitive marketplace for wireless and wireline broadband services.

Because the City receives a percentage of both advertising and fee-for-service revenue if certain revenue levels are exceeded by the EBK Wi-Fi business, it has injected itself as a competitor into the private market for wireless and wireline broadband services. As a consequence of its "competitor" status, the City is incented to administer, manage, and operate the EBK network to benefit expanding its market share, as any company would. The financial incentives are very powerful because as more and more people abandon existing offerings for Internet and Cable TV services for those provided by the free EBK Wi-Fi network, the City makes more and more money.

It is for this reason – the prospect of high revenue based on the percentage-based revenue sharing model - that the City could have decided to enter into the public-private monopoly Wi-Fi business partnership with Alphabet. It could have entered the market for this reason and not for the publicly stated reason to close the digital divide by serving the "over 25%" who lack broadband service. This is particularly true with respect to the fee-for-service revenue it would reap from the EBK network. Currently, the City only receives taxes on fee-for-service revenue generated by the wireless and wireline broadband market, but now it will receive 50% of the revenue of these services, plus the taxes.

So what the City could have done is to scheme with a private company, Alphabet (Sidewalk/Intersection), to offer a monopolistic Wi-Fi service for free basic broadband and fee-based value-added services in order to decimate the market for wireless and wireline broadband service.

This pricing model – free "basic" high-speed broadband service with fee-based value-added services – could wipe out all of the existing companies in the wireless and wireline broadband marketplace. The way this could unfold is as follows:

- 1) Establish a public-private partnership that offers a monopoly-based Wi-Fi broadband service that no other private companies can offer (because competitors don't own or have access to the public infrastructure – the sidewalks – on which the Wi-Fi units are installed).

The Stop LinkNYC Primer

- 2) Provide free “basic”, comparable high-speed broadband offering (40MB/sec per connection, with higher speeds at burst that can provide greater speeds, for free. The Franchise Agreement also encourages Alphabet to deploy higher broadband speeds for free).
- 3) Provide the high-speed broadband for free, supported by advertising fees that the public-private Wi-Fi monopoly displays through the EBK electronic display screen (which its competitors can’t do).
- 4) The free monopoly service encourages consumers to cancel their fee-based Internet services and siphons market share from existing wireline and wireless companies (which Alphabet and the City do through promotional advertisements on the EBKs electronic displays that say consumers can get free Wi-Fi through the network).
- 5) Consumers, once disconnected from their fee-based Internet services, use the EBK Wi-Fi monopoly network for value-added services, such as on-demand viewing of television shows, movies, video games, etc., which siphons off more revenue from fee-based Cable TV service providers. Consumers could “cut-the-cord” completely and cancel their Cable TV service, or become “cord nevers” and simply abstain from ever purchasing fee-based Cable or Internet and just use the free EBK Wi-Fi network. As news reports reveal on a consistent basis, more and more people are “cutting the cord” or simply never buying fee-for-service wireline broadband service. Both Alphabet and the City have read the tea leaves and know their monopoly Wi-Fi service – offering broadband for free – will attract an ever-increasing number of people.
- 6) The City receives both 50% of the revenue of the fee-based services and the taxes on them, as opposed to only the taxes. In addition, it receives 55% of the revenue generated by the monopoly broadband network’s advertising financial model. This revenue is or will be, presumably, greater than what it will reap in taxes on existing broadband services offered by wireless and wireline companies. In effect, the City becomes a de facto majority corporate owner of a monopoly Wi-Fi broadband service that could decimate the competitive marketplace. In the process of doing this, it will receive more than 50% of the total available market for high-speed broadband service.

The City has cleverly negotiated a minimum-fee contract with Alphabet in order to hedge an unfavorable outcome – that is to say, the outcome where the scheme just doesn’t work. The hedge is that the City requires a minimum payment of \$500 million over 12 years to ensure it gets some financial benefit from its corporate partnership with Alphabet. So, in the event people don’t move from their fee-based providers to the free monopoly EBK Wi-Fi network, the City will be able to represent to the public that it is receiving some financial benefit from its monopoly business venture that uses the peoples’ sidewalks. But its real goal could be to decimate the competitive market for broadband services provided by wireline and wireless companies. By doing this, it will reap very high revenue from its majority de facto ownership of the EBK Wi-Fi monopoly broadband network.

And this holds true for Alphabet as well, even as a minority owner of the public-private partnership (it will receive a little less than 50% of the public-private business’s total revenue after Year 7). If it can decimate the existing market for wireless and wireline broadband services, it will reap incredibly high revenue through its revenue-sharing agreement with the City.

The potential result of the City’s and Alphabet’s monopoly broadband Wi-Fi service could be the destruction of the competitive market for Internet and broadband service. The monopoly’s ability to price its high-speed broadband service below (its price is zero) the equilibrium price established by the competitive market could severely impact the financial viability of wireless and wireline companies. In addition, and importantly, the device metadata and other information Alphabet collects from the monopoly EBK network can be used to provide a higher level of advertising service in its Web services, which could harm the financial viability of competitors in those markets who compete for the same advertising dollars. Finally, the device data captured by the EBKs can be used to provide better targeting for advertisers who display ads on the EBKs, which would also siphon dollars away from other Web companies who rely on advertising fees for their revenue.

The Stop LinkNYC Primer

This type of economic rigging goes against the long-held economic principles of free and fair competition and fairness. Unless it's a natural monopoly, a monopoly not gained through skill, industry, and foresight in freely competitive markets are detrimental to society in the long-run. The monopoly that Alphabet and the City have on the provision of free broadband wireless Wi-Fi services is such a monopoly: it was not earned in the free market, but rather granted by the City of New York to both Alphabet and itself. It is also important to note that the EBK Wi-Fi monopoly is not a natural monopoly, where the lowest price, highest output, and greatest choice would manifest in the long run.

It also will be noted that this situation is not the same as reaping advertising revenue from city bus stands. In that situation the city has granted only itself – not a private company - a monopoly on providing local bus service. When it comes to the provision of broadband service, there is a robust competitive market with players such as Verizon, AT&T, T-Mobile, Comcast/Spectrum, and many others. What the City is involved with in this situation is providing a monopoly wireless Wi-Fi broadband service that: 1) can compete with existing Internet service and 2) is offered below the equilibrium price established by the competitive market by virtue of its sole ownership of the city's sidewalks.

The City and Alphabet May Have Colluded to Falsely Claim that “over 25% of New Yorkers Lack High-Speed Broadband Service” so They Could Decimate the Existing Competitive Market for Wireless and Wireline Broadband Services and Reap the Ensuing Financial Rewards.

The City and Alphabet claim that “over 25% of New Yorkers lack high-speed broadband at home”. The City, however, has not published any independent, statistically significant research that supports this claim. Moreover, the City has not provided any similar data on whether the reason for not having high-speed broadband at home is because people can't afford it or have technical access to it.

The only thing either the City or Alphabet has said in readily available public documentation is that:

*“Over 25% of New Yorkers lack high-speed broadband at home. LinkNYC [the EBKs] will address this glaring digital inequality **by making the fastest public Wi-Fi in the world freely available to millions of people for the first time. Many more will be able to reduce their spending on data plans.**”*

Both Alphabet and the City could have fabricated the “over 25%” number, using various data cobbled together in an unscientific manner or in a way that was not statistically sound or significant in order to justify the need for free Wi-Fi service. By inflating the number of people who, presumably, want high-speed broadband but can't afford it or get technical access to it, the public-private partnership provides the only justification for its deployment. If the number were smaller, then there would be no justification for even considering free high-speed broadband Wi-Fi service.

In addition, the claim does not define “who” a New Yorker is. Does it include only people who live in New York City or does it mean all people living in the state of New York? Does it include people who live in the City only part time? Does it include people who own a domicile but visit infrequently and therefore don't have a need for high-speed broadband? Does it include people living in the country illegally?

Certainly if the “over 25%” number includes all people living in New York state then there was a purposeful misleading of the public, which would need to be investigated by legal authorities. **The same is true if the “over 25%” number includes people living in the country illegally: citizens and lawful residents of New York City are not responsible for providing free, non-utility, discretionary high-speed broadband service to illegal immigrants and therefore they cannot be factored into an analysis on how many people don't have the service.**

The Stop LinkNYC Primer

The reason that both the City and Alphabet may have wanted to falsify the un-served population number is because of the amount of money each could make by decimating the established market for wireless and wireline broadband service. The City, as a majority owner of the EBK monopoly business in terms of revenue (it receives greater than 50% of the businesses revenue starting in Year 8), would reap a huge financial benefit from destroying the competitive market with its co-owned monopoly EBK Wi-Fi franchise. Alphabet's motivations, as previously discussed, are two-fold: 1) like the City, it could seek to destroy the competitive market for broadband services to reap monopolistic revenue, and 2) the EBKs will capture MAC Addresses and other metadata and personally identifying data that it can use to generate revenue in its other lines of business; for example, Google Search, Google Mail, Google Maps, AdSense, etc.

The general public, legal authorities, and regulatory agencies need to make the City account for its claim that “over 25% of New Yorkers lack broadband service” by demanding it provide the independent, statistically significant data it used to support the claim. This research must show that it was completed prior to the commencement of the process whereby it was decided free Wi-Fi service should be provided in all of New York City. This means that this data must have been known by the City well in advance to any public hearings on the franchise. The research for this data cannot be dated during or after the period of the public hearing process because it would be after-the-fact, which means it likely was falsified or manipulated to support the City's claim. And, the data supporting the City's claim cannot come from Alphabet, any of its subsidiaries, or other companies or firms that could financially benefit from the EBK Wi-Fi network. The only company from which the data can come is a reputable market research firm that has no prior or current business relationship with the City or Alphabet and which is not seeking to do business with either in the future.

The City Could Lose Tax Revenue and Jobs Because of the EBK Wi-Fi Network

Since one of the goals of the EBK monopoly business – and perhaps the primary one - is to siphon consumers away from fee-based wireless and wireline services, this could have a negative impact on the taxes raised by those services. If fewer people pay for these fee-based services then fewer taxes are raised by the City. Also, if companies lose business to the EBK Wi-Fi business, it will also cause unemployment since the established companies will need fewer employees due to their smaller customer base. Alphabet claims in its documentation that the EBK Wi-Fi business will create perhaps 200 jobs in New York, but did the City ever consider the number of jobs that will be lost if consumers switch from their fee-based service to the free monopoly Wi-Fi service? Did the City factor into its financial analysis the lower income taxes from those who lose their jobs? **The City needs to publish its financial analysis on the potential loss of tax revenue and employment due to its EBK business.**

Some questions:

- 1) Did the City conduct financial and employment analyses that took into account 1) lower tax revenue from reduced demand for services from wireless and wireline companies in the free market, 2) the loss of employment from those companies (and partners) due to lower demand for their offerings, and 3) the loss of income tax revenue due to the loss of employment?
- 2) Were these analyses discussed in the public hearing process?
- 3) Did the City do financial analyses that it did not make public because it would show a negative tax and employment impact?

Alphabet's Monopoly EBK Wi-Fi Service Allows It To Use Data To Anti-Competitively Cross-Subsidize Its Other Lines Of Business To The Financial Detriment Of Its Web Competitors

The device and personal data Alphabet captures through its EBK monopoly franchise can be leveraged in its other lines of business in competitive markets to provide targeted advertising that its competitors can't. Advertisers desire targeted ads because they provide a higher return on investment. As Alphabet collects billions and trillions of unique device and personally identifying data points from its EBK monopoly franchise, it can provide more granular and targeted advertising opportunities for its advertisers. This could have the effect of drawing advertisers away from competitors in various other lines of business in which Alphabet is a market participant, including markets for search, email, maps, ad serving, and others. This, of course, would lower the revenue for companies in those markets since their business revenue models rely primarily on advertising fees, and could possibly force them to cease operations. This would have the effect of reducing competition and possibly, in the long run, increasing prices that advertisers must pay for advertising on Alphabet's Web properties.

Alphabet Could Be Using its EBK Network as a Loss Leader in Order to Capture Mobile Device and Personally Identifying Information That it Could Use in its Web Businesses

Given that Alphabet generates 90% of its revenue from advertising fees, it is not unreasonable to assert that its EBKs may be a loss leader - a red herring of sorts - in order to capture device and personally identifiable information to generate higher advertising revenue in its other lines of business. It could look at its EBK network simply as a "cost of doing business" for these other market segments. **In this view, Alphabet might be willing to accept an operating or net loss in perpetuity on its EBK business as long as it can achieve a value greater than that loss from the use of device metadata, Web content and browsing information, and personally identifying information to generate higher advertising revenues in its other lines of business.**

Here's an example of how Alphabet could use unique device data captured by its EBKs to generate revenue for its Google Search and Google AdSense businesses with someone (Mary) looking to purchase an apartment in Manhattan:

- 1) Mary has been looking for an apartment to purchase and spends her Saturdays and Sundays visiting open houses.
- 2) Alphabet knows Mary's various locations on the weekends since its EBKs capture her unique device ID (MAC Address) through her Wi-Fi-enabled phone. Mary never uses the EBKs but does have her Wi-Fi enabled at all times.
- 3) Mary also has been regularly surfing real estate sites on the Web via her mobile device and home router. She finds sites to review by using Google Search, and she is logged into her Google account (from home) which has her personally identifying information, including her device's unique ID (MAC Address) since she is using an IPv6 device and her home Internet provider uses IPv6 for IP Addressing. IPv6 allows Alphabet to read Mary's MAC Address from Web server log files and through Packet Sniffing.
- 4) Currently, Alphabet has been displaying generic real estate advertisements to her via the Google Search page as well as through Websites she's looking at that contain information about places to live in the city.
- 5) To provide its real estate advertisers with more targeted information about Mary and her interest in real estate brokers, Alphabet runs an analytics software program that shows her visiting real estate websites and reading real estate articles from home using her mobile device.
- 6) Alphabet runs another analytics program that shows the EBK locations in Manhattan that captured her unique device ID (MAC Address) on the weekends and concludes - based on her search requests and physical location - she's looking for an apartment to purchase (**even though she never logged into any EBKs**).

The Stop LinkNYC Primer

- 7) Now, when Mary visits real estate sites while Web surfing at home, Alphabet sends a targeted ad from a real estate company that has specific properties to see in the Manhattan neighborhoods she visited.
- 8) **Mary has no idea this type of analysis and targeting is being done based on her geo-location and search requests. Importantly, she never logged into any EBKs and has no idea that Alphabet is using her location information – obtained from the EBKs capturing her MAC Address - to send her targeted real estate ads when she uses Google Search.**

Since Alphabet knows that Mary is looking for a place to buy and also knows the areas of the city she wants to live, it could charge a higher fee to its real estate advertisers - specializing in properties in the areas Mary is thinking of living – who show ads on its Web services like Google Search. Because Alphabet possesses her unique device data (MAC Address) captured via its EBKs – and already has her MAC Address in her Google account profile (obtained from her IPv6 Address) - it can provide real estate advertisers with a targeted advertising opportunity in its other lines of business.

What this means then is that the EBK network could be run at a loss since the MAC Address and other metadata it captures could be used to generate advertising revenue in Alphabet’s Web businesses. This additional revenue could possibly both 1) cover the operating and/or net losses of the EBK network and 2) provide higher profits for the company’s various Web businesses.

Alphabet also may achieve the same type of targeted advertising even if Mary did not log into her Google account that contains her personal information. If Mary’s IPv6 MAC Address is packet sniffed or read from Google’s log file when she submits her search request, Alphabet may be able to associate - on-the-fly - the mobile phone’s MAC Address with her personally identifiable information and send targeted real estate ads to her phone. Again, this is a scenario where Mary did not even log into her Google account.

Another example of how Alphabet could both monetize its EBK data and accept operating the EBK Wi-Fi network at a loss in perpetuity is illustrated by the following example:

Mike lives in Connecticut, commutes to his midtown Manhattan office for work, and regularly visits the NBA Store on 5th Avenue during lunch. The EBK installed on that block captures his mobile device’s unique ID each time he visits the store (he never logs into the EBK). At night he uses Google Search with his mobile device to look up basketball related articles and products. Alphabet uses a Packet Sniffer to either capture the IPv6 MAC Address of Mike’s mobile device, or reads it from the Google Search’s log file. Because Alphabet knows he is physically near the NBA store during lunch on a regular basis – via the unique device data (MAC Address) collected by its EBKs on the same block - it can display NBA ads to him in the search hit list. It could possibly charge the NBA higher advertising fees because it knows Mike is present near the NBA store quite often. It might be that Alphabet could have a dual advertising fee structure for the NBA: 1) a premium price for displaying ads to people who are known to be near the NBA store on a regular basis and 2) a standard price for everyone else.

The examples above illustrate the reason that Alphabet may be willing to operate the Wi-Fi network at a loss in perpetuity: it could make money in its other lines of business using the device metadata and personally identifying data captured by its EBKs. Given the massive profits Alphabet generates on an annual basis in its main businesses, it is not unreasonable to make this assertion. This monetization factor could provide the financial incentive for Alphabet to cross-subsidize its monopoly business with profits from its other lines of business to keep it solvent when it should be shut down due to its losses, or to the poor revenue performance that does not meet its Internal Rate of Return. And it is for this reason that State and Federal regulatory and legal entities need to evaluate the revenue and cost structure of the EBK network.

An Evaluation Must be Done on Alphabet's Cost Structure and its Revenues from EBK Advertising & Services to Determine if it's Operating the Wi-Fi Network at a Loss and Subsidizing its Monopoly Franchise with Revenue from its Other Lines of Business

Since Alphabet has been given a monopoly franchise (in partnership with the City) to provide broadband wireless Wi-Fi service in New York, Federal and State legal authorities must ensure that anti-competitive cross-subsidies are not being made to the EBK business from the company's other lines of business. In order to do this, Alphabet must provide to the City fixed and variable cost data for its EBK business as well as information on the advertising contracts and fee-for-service purchases that generate the revenue to fund the EBK Wi-Fi business.

If the information submitted shows that Alphabet is running the business at a loss, it may indicate that cross-subsidies are being made. Also, it may indicate that Alphabet is willing to run the EBK business at less than an acceptable profit, or even at a loss, in order to capture device metadata and personally identifiable information that it could use to generate revenue in its other lines of business.

In addition to providing revenue and cost data to the government, Alphabet also needs to provide it to non-governmental groups. These entities include privacy rights organizations, public financial watchdog groups, economic research firms, and accounting firms. All of these non-public entities must be non-partisan and have no past, present or future business relationship with either the City or Alphabet. If no non-partisan entities can be found, then an equal number of partisan entities must be retained in order to provide a check-and-balance on each other.

The information that Alphabet needs to provide is as follows:

- 1) hard copies of the signed contracts for EBK advertising that contain the amounts to be paid to Alphabet by companies showing their ads, including purchase orders, invoices, and receipts.
- 2) purchase orders, invoices and receipts that would verify the revenue generated by EBK pay-services.
- 3) data on capital costs, annual operating costs, fixed and variable costs for each physical component of the EBK network, and fixed and variable costs for all non-physical components (personnel costs, royalty payments, non-network facilities, etc.).
- 4) financial models used to evaluate the EBK business.
- 5) Internal Rate of Return (IRR) data the company uses in its financial models.

The reason cost, revenue, and Internal Rate of Return information are needed so an assessment can be made on whether Alphabet is cross-subsidizing its EBK operation with profits from its other lines of business. If it is, this could be deemed an anti-competitive or anti-trust violation since it would allow the company to provide its monopoly Wi-Fi broadband service only by funding it with profits from its other lines of business (see further discussion in separate section below). This cross-subsidy would allow it to maintain itself as a "going concern" – and offer its services to consumers at a predatory price of zero – when in fact it should be shut down and terminated.

Alphabet is already in the situation where its monopoly use of public lands (the sidewalks) to operate its business (both EBK advertising and EBK Wi-Fi service) allows it to undercut the equilibrium price established by the competitive market. The price it charges customers is zero while its competitors must charge monthly fees for their wireless and wireline Internet and broadband services. While this monopoly pricing scheme – in existence only because of its public-private monopoly business partnership with the City – is, in and of itself, detrimental to the competitive market, if it's the case that the EBK operation is losing money then Alphabet must be subsidizing it with profits from its other businesses. If it weren't able to do this cross subsidy, the EBK network would not be able to operate as a going concern and would have to shut down.

Alphabet Can Make it Appear it is Generating Ad Revenue From its EBKs by Cross-Subsidizing Revenue From its Web Services Business to its EBK business.

It's possible for Alphabet to provide cross-subsidies to its EBK network from its traditional line of web services such as Google Search, Gmail, Google Maps, and others. There are two ways this could be done:

- 1) Alphabet could have a contractual agreement with its advertisers that provides EBK advertising for free if a company purchases a set amount of ads for other lines of business that it owns. For example, Alphabet might say that if an advertiser spends \$5,000,000 for ads on its Google Search and Google Maps businesses, it will also show the ads on its EBKs for free. So, to an advertiser, the cost of advertising on the EBK network would be zero, which also means that Alphabet would be bringing in no revenue. This, in turn, means Alphabet would have to anti-competitively subsidize its EBK monopoly franchise with profits from its other lines of business in order for the Wi-Fi network to continue operations. Because this is a very real possibility, an evaluation of Alphabet's advertising contracts must be done to ascertain whether it's actually charging fees for ads displayed on its EBKs or providing this service for free in conjunction with ad purchases tied to other businesses it owns.
- 2) Another way Alphabet can make it look like it's generating ad revenue from its EBKs when it really isn't is where it provides free or discounted advertising on its web services properties (e.g. Google Search, Gmail, and Google Maps) when ads are purchased on the EBK network. Alphabet could do this in order to show regulators that it's generating ad revenue from its EBK network in order to demonstrate that it is a self-sustaining business. But this would merely be an accounting gimmick to evade scrutiny by regulators as to the viability of the EBK business as a going concern. To the advertiser, it doesn't matter whether the ad expense is allocated to Alphabet's EBKs or other web properties: all it cares about is the number of impressions it will get for both. If it's going to get one million ad impressions on the web service properties for free because it purchases EBK ads then that would be perfectly fine. The advertiser doesn't care how Alphabet accounts for the fees charged, it only cares that it receives an acceptable number of ad impressions. Here's how it could work:
 - An advertiser has spent \$200,000 a year on Google Search and Gmail for the past five years. Each purchase provides one million ad impressions annually.
 - Alphabet tells advertisers that if they take the \$200,000 and spend it on EBK ads going forward, it will provide one million ad impressions on Google Search and Gmail – or other web services it owns - for no cost.

So, for its \$200,000, the advertiser continues to get one million ad impressions on Google Search and Gmail, as well as the ad impressions on the EBK network. The advertiser doesn't really care how Alphabet is accounting for the expense...that's Alphabet's internal business concern. The advertiser's only real concern is that it continues to get the one million ad impressions on Google Search and Gmail and, "Hey, if we get ads on the EBK network then that's cool too". What Alphabet gets out of this accounting slight-of-hand is the ability to show regulators that its monopoly EBK network is generating revenue and is not being subsidized by its other business services. But this would just be an exercise in accounting gymnastics, since there is a de facto subsidization taking place given that the EBK revenue is being generated **only because** Alphabet is taking a \$200,000 loss on the one million ad impressions it promises to deliver for the advertiser – and has historically delivered to it - on Google Search and Gmail. This type of subsidy is anti-competitive and allows Alphabet to provide monopoly broadband Wi-Fi service below the equilibrium price established by the competitive wireless market. Because of this anti-competitive subsidy, Alphabet can provide its monopoly broadband Wi-Fi service for free, while wireless cell carriers must charge a fee for its service (typically between \$40 and \$100 month per user).

The City Needs to Require Advertisers to Provide Return on Investment Data for its EBK Advertising

Regulators must require companies who advertise on the EBKs to provide statistically significant data generated by marketing/advertising feedback surveys – executed with people living lawfully in New York City and who are at all income levels - to see if their EBK ads are effective and something for which they will continue to pay. In particular, the survey needs to be executed with people living in areas where the vast majority of the “over 25% of New Yorkers who lack high-speed broadband” live. Again, it cannot include people living in the country illegally: lawful residents of New York City are not responsible for providing high-speed broadband service to illegal immigrants.

The contracts and payments for the EBK ads cannot be co-mingled with other advertising services for which companies may also contract with Alphabet. The feedback survey must be executed by a third party marketing vendor and include standard industry questions and topics that these types of surveys include, particularly around advertising recall, response, and persuasion.

There are established industry methods to do advertising feedback research and the City must require that companies advertising on the EBKs conduct them on a bi-annual basis with an unbiased marketing vendor. The population to survey must be that which lives around the EBKs, are legal residents, and must be executed either by phone or in-person “on the street” interviews. People who do not live in New York City can’t be used as survey respondents since the justification for the network in the first place was to provide free broadband wireless Wi-Fi service to the “over 25% of New Yorkers” who lack it. The surveys must include contact name, contact phone, and contact address so follow-up calls can be done by an independent, non-City entity to audit the feedback results. This will ensure no falsifications were done in the execution of the survey.

It is critical that the City require the marketing feedback survey to be conducted on a bi-annual basis. This will allow the public the ability to ascertain whether the ads are effective for the companies advertising on the EBK network. By not executing the feedback survey, the City will not know whether company advertising contracts with Alphabet are paying for EBK advertising or for advertising in other business areas that Alphabet owns, such as Google Search or Google Mail. In other words, Alphabet could offer to its advertisers a “run-of-properties” type of advertising model where its ads are displayed on multiple Alphabet properties for a set contract price; for example, one contract could provide display ad impressions on the EBKs, Google Search, Google Mail, and Google Maps. **A company advertising on Alphabet’s various businesses may be willing to accept this “run-of-properties” model without really evaluating the effectiveness – that is, the return on investment - of the specific EBK ads. A company may be willing to forgo the analysis because it’s costly to execute feedback surveys with people, which is the only way it could measure its return on its EBK investment. Meanwhile, it can get very good feedback on the advertisements it has on Alphabet’s Web properties because it can look at standard industry metrics such as click through rates and form fill outs.**

An Independent Board is Needed to Manage the Feedback Survey

In order to ensure that neither the City nor Alphabet bias the feedback survey with advertisers, an independent board needs to be established that will create and manage the effort. The board needs to be comprised with representatives from the following entities:

- Civil Rights Group
- Privacy Rights Group
- Border Control Group (to ensure illegal immigrants are not included)
- NYC Community Boards
- Technical Lab
- Market Research Company (which would create and execute the feedback survey)

The Stop LinkNYC Primer

The market research company can have no prior, current, or future relationship with either the City or Alphabet. It must lead all aspects of the survey, including development, execution, tabulation, and reporting. Alphabet can have no role in the survey effort other than to provide a complete list of all advertisers on the EBK network and, if needed, copies of the advertisements. The City can have no role in the survey at all other than to provide all the funds for the research.

Elements to Measure Advertising Effectiveness

The advertising feedback survey needs to be performed to ensure that Alphabet's advertising customers are actually paying for EBK advertisements. No company would advertise on the EBKs if there weren't a financial return on its investment (even branding must ultimately be associated with a return on investment). The three methods that companies typically use to test advertising effectiveness are response, recall, and persuasion:

Response: this tests an advertisements ability to initiate an action by the person who sees it. Examples are: calling a phone number that is displayed, sending an email to the company inquiring about its product or services, going to a website to get more information, and clicking on a web link.

Recall: this tests an advertisements ability to be memorized and then recalled by a person. It is used primarily to see if the ad had the effect of "branding" a product or company in the person's mind.

Persuasion: this tests an advertisements ability to change a person's view. It tests for a person's view of a product or company before and after an advertisement is seen.

Why an Advertising Feedback Survey is Necessary

It is important for the City to require advertising feedback tests because if the results are low or bad for the advertisers it means they will not pay to advertise on the EBKs. If they don't pay Alphabet for advertising on the EBKs, then the company can't generate enough revenue to cover its fixed and variable costs. This in turn would mean Alphabet must anti-competitively subsidize its monopoly franchise EBK Wi-Fi business with profits from its other lines of business. This subsidy would allow the monopoly EBK Wi-Fi business to continue to offer free wireless broadband service - below economic costs - which in turn would allow it to continue to compete against its fee-for-service wireless and wireline competitors when it otherwise should be shut down.

In other words, if Alphabet can't generate the revenue from its EBK advertising (and value-added services) to achieve the company's Internal Rate of Return, then the EBK Wi-Fi service operation should be terminated from a corporate finance perspective.

But Alphabet could want to keep the EBKs in operation since it can monetize the millions, billions, and trillions of data points the units capture in its other lines of business; that is, the device metadata, usage data, location data, and personally identifying data captured by the units. Alphabet may be willing to continue to operate the EBK network even though it cannot cover its costs and does not achieve its Internal Rate of Return because the monetized value of the EBK data in its other lines of business is higher than the costs of running the Wi-Fi network.

In summary, the entire EBK Wi-Fi business could be a red herring and a loss leader for Alphabet: the company may be willing to take losses – and steep ones at that - in perpetuity so it can monetize the value of the device, usage, location, and personal data its EBKs capture from users and non-users in its other lines of business. And, because as a money-losing business it does not have sufficient profits or revenue to pay the fees under the Franchise Agreement, it would be using funds generated from its other, profitable Web businesses to cross-subsidize its free EBK monopoly Wi-Fi business. This would have the effect of anti-competitively undercutting the competitive equilibrium price established by the wireless and wireline fee-for-service markets, and ultimately harm existing market participants or drive them out of business.

Alphabet's Market Dominance and Power for Cell Phone Operating Systems - as Defined by the Herfindahl-Hirschman Index – Allows it to Force Wi-Fi to be Enabled in New Mobile Device Activations

A major anti-trust issue that could arise with the EBK Wi-Fi network is due to the tie-in between Alphabet's ownership of the monopoly franchise and its market dominance and power in cell phone operating systems. The Wi-Fi monopoly it has been granted by the City utilizes the public sidewalks and no other company has been given the right to provide the same service. While the Franchise Agreement says that the contract is non-exclusive, the fact is that Alphabet is the only company allowed to install EBKs, so it is a monopoly.

The dominance and power it has in the cell phone operating system market is that it has a market share of 85.2% (Gartner Group, August 2016) and the entire market is very concentrated. According to the Herfindahl-Hirschman Index (HHI), the mobile phone operating system market is highly concentrated because the index's value is over .25, or 25% (which is the HHI's minimum level for market concentration)

As of August 2016, Gartner Group estimates that Alphabet's Android and Apple's iOS mobile operating systems comprise 99% of the market for new device shipments. For the calendar year 2016, Gartner estimates that new shipments with the Android operating system will be 85.2% and new shipments with iOS will be 13.8%. The Herfindahl-Hirschman Index (HHI) provides the following result based on the following company market shares:

.852 for Android
.138 for iOS
.008 for Blackberry*
.001 for Microsoft *
.001 for Samsung*

* In November 2016, the market research firm Strategy Analytics claimed that Blackberry, Microsoft, and Samsung accounted for 1% of the mobile phone operating system market, which has been allocated for this analysis as indicated above.

HHI Calculation: $.852^2 + .138^2 + .008^2 + .001^2 + .001^2$

HHI Result = $.725904 + .019044 + .000064 + .000001 + .000001 = .745015$ (about 75%)

The result .745 is well above the U.S threshold for market concentration, which is .25; thus, the mobile phone operating system market is highly concentrated. And Alphabet's 85.2% market share means that it has a high level of market power and dominance.

What Alphabet is able to do with this market power and dominance is to force cell phone hardware manufacturers to install its Android operating system with Wi-Fi configured to be enabled – that is, turned on - upon initial device activation. This means that consumers of Android mobile devices would be forced to divulge their unique device IDs (MAC Addresses) to Alphabet's EBKs upon initial activation of a device. This, in turn, would mean that Alphabet would know where an individual lives down to the block or building in New York City, since 99.99% of people activate their new mobile devices from home. Since the EBKs can capture mobile device Wi-Fi signals within a 150 to 400 foot radius, they will be able to capture almost all new phone activation in New York City and locate its owner's residence down to the block or building. **Importantly, Alphabet also will be able to force consumers to be tracked throughout New York City because its EBK network will capture their devices' MAC Addresses everywhere they go.**

To re-iterate, Alphabet can do this because its market power and dominance can influence or force cell phone hardware manufacturers to ship Android devices with Wi-Fi enabled. Once a phone is activated, it will automatically transmit its unique device ID (MAC Address) to an EBK, either from the home where the activation took place or when someone takes it outside for the first time. Since an EBK will capture the unique device ID

The Stop LinkNYC Primer

upon initial activation, Alphabet will know that a person lives on a specific block. All Alphabet needs to do in order to determine this is to run a simple analytic software program for its EBKs that lists all MAC Addresses in order from the time they were captured. By cross-referencing all of these lists, Alphabet can determine which EBK first captured a unique device ID. From this, Alphabet knows that a person lives on the block where that EBK is located. It could also pinpoint the specific building the person lives in. **The reader is reminded that this very specific information is being captured for people who don't even use EBK Wi-Fi service.**

Alphabet's Market Power in Mobile Phone Operating Systems Allows it to Not Include MAC Address Randomization as a Capability.

Because Alphabet has such extreme dominance in the cell phone operating systems market, it is not subject to competitive forces for integrating any particular technical capabilities or features. This means that the company could unilaterally decide not to include privacy features that the market demands either because of cost concerns or because they could reduce its ability to generate revenue for its digital advertising model. One of the technologies that would impact its digital advertising revenue is MAC Address Randomization, which provides a higher level of privacy and anonymity to devices (and people) than a single, unique MAC Address. See Definitions and Terminations section for further explanation.

MAC Address Randomization may make it more difficult for Alphabet to associate a device with all of its metadata and personally identifying data because there no longer would be one unique device ID per device – it would have multiple IDs. This would make it difficult – though not impossible – for Alphabet to track the usage of any single device, which would impact its ability to deliver targeted digital ads. With less targeting of its ads, it cannot charge advertisers the higher fees that it could with a higher level of targeting. Ultimately, MAC Address Randomization would lead to lower revenue for Alphabet unless it was able to associate the multiple MAC Addresses to one specific device. It might be able to do this by knowing all of the MAC Addresses that could be generated by any single device. But if it could do that, then it would defeat the purpose of having MAC Address Randomization in the first place and the integration of this capability would serve only as a ruse to consumers.

Due to its Monopoly Franchise and Market Dominance in Cell Phone Operating Systems, Alphabet is the Only Company in the World That Will Have the MAC Addresses of All People In New York City. This Gives it an Unfair Competitive Advantage and Creates a Serious Privacy Issue.

Because of Alphabet's Wi-Fi monopoly and its dominance in cell phone operating systems, it will be the only company in the New York City market that will be able to capture MAC Addresses of all Wi-Fi enabled devices and products. This gives it a huge competitive advantage over its competitors in the markets for broadband Internet and Web services. Since it will be the only company to have metadata and MAC Address information on devices and products, it can use it to provide more targeted advertising to advertisers. This could have the effect of advertisers moving away from competitive Web services (to Alphabet's Web services) since they are getting a higher return on their advertising investments with Alphabet. This could have the effect of reducing Alphabet's competitors' advertising revenues to the point where they cannot provide their services and must shut down. This would be anti-competitive because it is by virtue of Alphabet's monopoly Wi-Fi service that it's amassing the data and metadata that's ultimately being used to siphon off advertising dollars from its competitors' Web businesses. In addition, it also would be anti-competitive if Alphabet is cross-subsidizing its EBK Wi-Fi business with revenue from its Web services businesses. This cross-subsidy would allow the EBK business to remain in operation when it should be shut down due to losses or low profitability that does not meet its Internal Rate of Return.

Ethics and Corruption Issues

An investigation should be conducted into the City's process for selecting and awarding the LinkNYC EBK franchise to provide free broadband Wi-Fi in New York City. This investigation should be done by State and Federal legal and regulatory authorities, with the assistance of non-profit government watchdog groups. The specific areas that should be focused on are:

- 1) The claim that "over 25% of New Yorkers lack high-speed broadband service".
- 2) The decision process and rationale used by the City to award only one company a monopoly franchise to provide Wi-Fi service.
- 3) The rationale for not publishing a Request for Proposal so that multiple companies could bid on the franchise.
- 4) The roles that former City of New York employees – who later became employees of Alphabet/Sidewalk/Intersection - may have played in the City's: a) decision to deploy free broadband Wi-Fi and b) the choice of Alphabet/Sidewalk/Intersection/CityBridge as the monopoly franchise.

There is No Independent, Statistically Significant Data Published by the City to Support its Claim that "over 25% of New Yorkers Lack Highspeed Broadband Service"

Alphabet (and the City) claim that "over 25% of New Yorkers lack high-speed broadband service. From Alphabet's marketing material on its website in 2016:

*"Over 25% of New Yorkers lack high-speed broadband at home. LinkNYC [the EBKs] will address this glaring digital inequality by making the fastest public Wi-Fi in the world freely available to millions of people for the first time. **Many more will be able to reduce their spending on data plans.**"*

As noted previously in other sections of this document (see Monopoly section), but will be repeated here, no independent and statistically significant data has been provided to the public or published by either the City or Alphabet to verify their claims that "over 25% of New Yorkers lack high-speed broadband service". There is no definition around this fuzzy claim, which presumably means that the people referenced want high-speed broadband but either don't have technical access to it or can't afford it. There are a number of issues with this claim, which is the sole justification cited by Alphabet and the City for deploying the LinkNYC EBK Wi-Fi network:

- 1) How did the City determine the "over 25%" number? Did it conduct a randomized, statistically significant survey of residents lawfully residing in New York City? Did it request data from existing wireline and wireless carriers? Did the City rely on data provided by Alphabet, which had the financial interest in justifying a high number so it could win the franchise? If it did the latter, the City committed malfeasance in its due diligence since it relied on a biased source – a source that would financially benefit from the data - for the quantitative data used to justify deploying the Wi-Fi network.
- 2) The City does not define "who" a New Yorker is. Does it include only people who live in New York City or does it mean all people living in the state of New York?
- 3) Does it include people who live in the City only part time and don't want broadband service in the home?
- 4) Does it include people who own a domicile but visit infrequently and therefore don't have a need for high-speed broadband?
- 5) Does it mean a person or a household unit?
- 6) Does it include people living in the country illegally? If so, why are legal residents and citizens responsible for providing a free broadband Wi-Fi non-utility service to them (or any communications service)?

The Stop LinkNYC Primer

- 7) Does it include people who are physically or mentally unable to use technology at all, such as elderly people with cognitive issues, or those with physical and cognitive conditions that also make it impossible for them to use technology?
- 8) Does it include the homeless or those living in half-way houses? If so, did the City determine how many have Wi-Fi devices so they could access the EBK Wi-Fi service through them? The City could not have included this population with the idea that they would access high-speed Internet from the EBK units themselves since the Franchise Agreement specifies that the units must be accessed only by Wi-Fi devices (and, since the Web browser functionality has been disabled, the population who accessed the Wi-Fi through the units themselves no longer matters).

The high percentage of “over 25%” is the only reason that the City has offered as justification for deployment of a free Wi-Fi network in the five boroughs. Consumer watchdog groups as well as State and Federal government legal entities need to investigate this claim by the City and demand it source the independent, statistically significant market research on which it relied to justify the Wi-Fi network. “Independent” means research that was previously commissioned by the City from a market research firm that had no previous, current, or future business with either the City or Alphabet, or any entity that would financially benefit from the EBK Wi-Fi network. If it cannot do this, then the City was either grossly negligent in its market research and due diligence efforts or it flat out lied to the public regarding the need for a free Wi-Fi network.

In addition, a randomized survey needs to be done with those who lack broadband access at home or through their mobile devices. The objectives of this survey would be to see:

- 1) If people get, and are satisfied with, free broadband service offered by commercial establishments such as coffee shops, restaurants, hotels, etc.
- 2) If people simply don't find high-speed broadband useful either for their home or their mobile device. Contrary to what the City and Alphabet may think, not everyone is hooked on the Internet or finds it fun, informative, and useful. There may be many reasons why people don't purchase broadband service that have nothing to do with affordability. For example, a family may not want its children to use social media sites or access pornography or waste their time in a digital world. Or, they may not want to subject their computing devices to viruses that can damage them and force the purchase of a new one.
- 3) If elderly or disabled people don't want it because they have physical or cognitive conditions that make them not want to use broadband.
- 4) If some people just don't have an interest in the Internet or broadband video for whatever reasons they say.

So, even if “over 25% of New Yorkers” (lawful residents only) lack high-speed broadband”, there may be valid reasons why many of them don't have it that have nothing to do with cost or being able to get technical access to the service. **If the City can't provide a sound methodology that was used to produce independent and statistically significant data, it would be clear it either fabricated the “over 25%” claim or used biased data provided by parties who had an interest in seeing the Wi-Fi network deployed. And this would provide evidence that the reason for deploying the network had nothing to do with serving a large, disadvantaged community but everything to do with generating revenue for its monopoly public-private business partnership with Alphabet.**

For Alphabet, the benefit of the false claim would be an opportunity to: 1) generate revenue from an advertising-supported wireless service that could siphon off customers from wireline and wireless providers – and perhaps put them all out of business, and 2) capture billions and trillions of data points from Wi-Fi devices (via MAC Addresses and other metadata) that it could use to generate revenue in its other lines of business. For the City, the benefit of the false claim would be the revenue it would reap from its revenue-sharing model with Alphabet where it collects 55% of digital ad revenue and 50% of fee-for-service revenue. As Alphabet makes more and more

The Stop LinkNYC Primer

money due to consumers dropping their wireless and wireline carriers' fee-based services, the City makes more and more money too. Also, Alphabet can use the device data and personally identifiable information it captures and derives from its EBKs and other businesses to provide more targeted ad opportunities for its EBK advertisers. Ads that are more targeted will provide higher revenue to the company, as well as to the City.

The City's Geographic Deployment Strategy of the Required 7,500 EBK Wi-Fi Units Cannot be Reconciled with the Claim That "Over 25% of New Yorkers Lack High-Speed Broadband Service"

As previously noted in this document, the deployment of the required 7,500 EBK Wi-Fi units does not make sense if its primary intent is to serve the "over 25%" population that the City and Alphabet claim lack high-speed broadband service. The Franchise Agreement's SRV Attachment shows how the two are putting the majority of EBK units in the wealthiest borough, Manhattan, where the fewest of the "disadvantaged 25%" live. In fact, while Manhattan makes up about 17% of the city's population, it will get 52% of the required units (3,900), all of which will have advertisements. SRV Attachment Section 1.2.3 (viii) shows the rollout of the required 7,500 Wi-Fi units (by Year 8 of the contract) as follows:

	Number of Wi-Fi Units WITH Advertising	Number of Wi-Fi Units WITHOUT Advertising	Percentage of Units
Brooklyn	767	579	18%
Bronx	361	375	10%
Manhattan	3,900	0	52%
Queens	943	296	17%
Staten Island	29	250	4%
Total	6,000	1,500	

This data is a critically important point to understand, since both Alphabet and the City make the claim that the primary reason to have free wireless broadband service is to serve the "over 25% of New Yorkers who lack high-speed broadband service" and, in their words, "to close the digital divide". By installing a majority of EBKs in all of Manhattan, it is doing exactly the opposite of what it should be doing, which is to install them in the poorest boroughs and areas of the city. Clearly, citing the "over 25%" is important to Alphabet and the City insofar as winning and awarding the monopoly franchise but not in actually providing the service to this population. It does not take a rocket scientist to know that 52% of the "over 25%" do NOT live in Manhattan, yet this borough will receive this percentage of the required 7,500 Wi-Fi units. Even if the additional 2,500 optional units are deployed in the other four boroughs, Manhattan would still have 39% of the units. And this would be far above the percentage of people who "lack" high-speed broadband in this borough. Since Manhattan has around 17% of the city's population, it at most should be receiving that percentage of the required EBK units, around 1,700; that is, assuming it has a proportionate number of the "over 25%" to the other boroughs. It is likely, however, that Manhattan has a lower number of the "over 25%" population, so it should be receiving even fewer units. Does anyone truly believe that even one person in the "over 25%" population lives between Madison and 5th in Midtown Manhattan between East 60th and 66th streets? Why are EBKs being deployed there, or in any wealthy area of the city?

The Franchise Agreement’s Geographic EBK Deployment Strategy Does Not Comport with the Land Area of NYC’s Boroughs & Population, Which Makes it Illegal and Also Unconstitutional

The geographic deployment of the required 7,500 EBKs is discriminatory as well as illegal since it does not align with the stated goals and justification by the City to provide Wi-Fi service to its residents, in particular the “over 25% of New Yorkers who lack high-speed broadband”. It is also a violation of the “equal protection” clause of the Constitution’s 14th Amendment (see the Privacy section’s Constitutional Issues discussion for further detail). This discriminatory deployment strategy is revealed by analyzing where the EBKs are required to be installed and comparing the number of them with the square mileage of the land area of the five boroughs.

The land area of the five boroughs of New York City is 304 square miles. Manhattan has 23 square miles of this total, or only 7%. So, while Manhattan is 7% of the land area it receives 52% of the EBKs (or 39% if the additional 2,500 units are deployed in the other four boroughs). And to reiterate, it has only 17% of the population. This clearly does not comport with the justification for a free public Wi-Fi network in order to, as the City and Alphabet claim, “close the digital divide” for “the over 25% of New Yorkers who lack high-speed broadband service”.

Land Area Analysis of New York City

Borough	Land Area (Square Miles)	Land Area % of New York City
Manhattan	23	7%
Bronx	42	14%
Staten Island	59	19%
Brooklyn	71	23%
Queens	109	36%
Total	304	100%*

* Rounded

Splitting the square mileage for the city between Manhattan and the other four boroughs, the density of deployment of both EBK advertising and non-advertising Wi-Fi units looks like this:

Manhattan: 170 units per square mile

This is derived from 3,900 EBK units divided by the 23 square miles that comprise Manhattan (with all 3,900 EBKs displaying ads).

Other Four Boroughs Combined: 13 units per square mile

This is derived from 3,600 EBK units divided by 281 square miles that comprise the other four boroughs (with 2,100 EBKs displaying ads and 1,500 EBKs without ads).

If the optional 2,500 units are deployed in Manhattan the density **is a whopping 278 EBK units per square mile.** If the additional 2,500 units are deployed in the other four boroughs, the density **is only 22 EBK units per square mile** for the areas outside of Manhattan.

So, as we see, the deployment density of the 3,900 required EBKs in Manhattan translates to 170 units per square mile versus 13 units per square mile in the other four boroughs combined. And it means Manhattan will receive 13 times (170 divided by 13) the number of units per square mile than the other boroughs combined. In terms of percent, this means Manhattan has a deployment density per square mile that is 1,200% higher than the other

The Stop LinkNYC Primer

boroughs combined. **To make this more concrete, there will be – for example - 170 EBK electronic advertising units from 60th to 80th streets between approximately 1st and 5th Avenues. This is absolute insanity.**

And, for EBKs that display advertising, it’s even worse for Manhattan. All of Manhattan's 3,900 EBKs are required to show advertisements while only 2,100 units are required to show them in the other four boroughs combined. So, from an EBK advertising perspective, the density ratios are as follows:

Manhattan: 170 units per square mile will show electronic advertisements.

Other Four Boroughs Combined: only 7 units per square mile will show electronic advertisements (2,100 units divided by 281 square miles).

So, Manhattan has 24 times the number (170 divided by 7) of EBK advertising structures per square mile as the other four boroughs combined. That translates to a 2,300% higher density per square mile in Manhattan for advertising units than the other four boroughs combined.

The following tables summarize this analysis and provide additional data on how discriminatory the EBK deployment strategy is and why it is illegal since it 1) violates the City’s justification for providing free Wi-Fi service to “the over 25% of New Yorkers who lack high-speed broadband service” and 2) violates the Federal Constitution’s 14th Amendment’s equal protection clause for the residents of Manhattan (in the context of #1).

EBK Deployment Density of the Required 7,500 Advertising and Non-Advertising Units

Borough	Units	% Units	% of Total Units Requiring Ads	% of Total Advertising Units	% of Land Area	% of Population	EBK Units (Per Square Mile)	EBK Ad Units (Per Square Mile)
Manhattan	3,900	52%	52%	65%	7%	17%	170	170
4 Boroughs*	3,600	48%	28%	35%	93%	83%	13	7
Total	7,500	100%	80%*	100%	100%	100%	n/a	n/a

* Bronx, Brooklyn, Queens, Staten Island

** Only 2,100 of the 3,600 EBKs in the other four boroughs are required to display advertisements, while all units in Manhattan are required to display them.

EBK Deployment Density of 10,000 Advertising and Non-Advertising Units (with an additional 2,500 optional Advertising units in Manhattan only)

The Stop LinkNYC Primer

Borough	Units	% Units	% of Total Units Requiring Ads	% of Total Advertising Units	% of Land Area	% of Population	EBK Units (Per Square Mile)	EBK Ad Units (Per Square Mile)
Manhattan	6,400	64%	64%	75%	7%	17%	278	278
4 Boroughs*	3,600	36%	25%	25%	93%	83%	13	7
Total	10,000	100%	89%**	100%	100%	100%	n/a	n/a

* Bronx, Brooklyn, Queens, Staten Island

** Only 2,100 of the 3,600 EBKs in the other four boroughs are required to display advertisements, while all units in Manhattan are required to display them.

EBK Deployment Density of 10,000 Advertising and Non-Advertising Units

(with an additional 2,500 optional Non-Advertising units in the other four boroughs)

Borough	Units	% Units	% of Total Units Requiring Ads	% of Total Advertising Units	% of Land Area	% of Population	EBK Units (Per Square Mile)	EBK Ad Units (Per Square Mile)
Manhattan	3,900	39%	39%	65%	7%	17%	170	170
4 Boroughs*	6,100	61%	21%	35%	93%	83%	22	7
Total	10,000	100%	60%**	100%	100%	100%	n/a	n/a

* Bronx, Brooklyn, Queens, Staten Island

** Only 2,100 of the 6,100 EBKs in the other four boroughs are required to display advertisements, while all units in Manhattan are required to display them.

In conclusion, the deployment strategy for the EBK units DOES NOT COMPUTE with respect to the square mileage land areas of the five boroughs. And it does not compute with the overall population of New York City or with respect to the “over 25% of New Yorkers” who the City and Alphabet say “lack high-speed broadband service” and to their claim of wanting to “close the digital divide.

The deployment strategy doesn’t compute for primarily two reasons (there are others as well):

- 1) The deployment of the LinkNYC network actually has little to do with serving the "over 25%" population or all residents of the city but mostly with Alphabet's and the City's desire to show advertisements – on 3,900 EBKs, and perhaps more - to the millions of people who visit, commute, or live **in Manhattan** every day. The people whom the public-private partnership is targeting with their ads are from the other four boroughs, the New Jersey/New York/Connecticut Tri-State area, other States, and other countries (tourists and business travelers). The more people to whom Alphabet can show advertisements, the more money it makes. And the more money it makes, the more money the City makes since it has a variable revenue sharing contract that gives it 50% of advertising revenue from years 1 thru 7, and then 55% of advertising revenue from year 8 through 15. There are fewer Wi-Fi units in the other boroughs – and fewer of them requiring advertising – because the mass of people (City residents, commuters, and visitors) don’t go to those areas....**they go to Manhattan.**
- 2) Alphabet benefits from the mobile device and home computer data and metadata its EBKs capture. Alphabet can monetize the geo-location metadata, device metadata, EBK usage data, its website log file data, and its AdSense advertising data in the operation of its EBK and Web businesses. This could be the most important aspect of the business to Alphabet.

So, to sum up: even though Manhattan:

- a) contains only 17% of New York City’s population,
- b) has a smaller percentage of the “over 25% of New Yorkers” who “lack high-speed broadband service” compared to each of the other four boroughs, and
- c) comprises only 7% of the physical land area of the five boroughs,

it will:

- a) receive 52% of the total number of required LinkNYC EBKs,
- b) receive between 65% and 75% of EBK advertising units (of the number required to display ads), and
- c) have a deployment density, at minimum, of 170 EBK units per square miles versus 13 units per square mile for the other four boroughs combined. If just considering advertising units, this number drops from 13 to only 7 units per square mile for the other four boroughs. If the 2,500 optional EBK units are deployed in Manhattan, the density increases to 278 EBK units per square mile, and the same number holds if they display ads.

The Stop LinkNYC Primer

Notwithstanding the issues pertaining to the blight and visual pollution created by the total number of EBKs and the number of them with electronic advertisements in Manhattan, legal and regulatory authorities as well as investigative reporters can plainly see that the numbers do not compute with respect to serving the “over 25%” population, or even serving all of the city in an equitable fashion. These numbers also don’t compute with respect to the EBK deployment density per square mile in Manhattan versus the other four boroughs, including the percentage that will display electronic advertisements.

Action Item for the Government and Media

Legal, regulatory, and media investigations need to be conducted regarding the incongruity between the City’s and Alphabet’s justification for deploying a free Wi-Fi network in New York City and the actual geographic deployment strategy of the units, including those that will display electronic advertisements.

Competitive Bidding Process

Another question that is raised by the public-private business partnership between Alphabet and the City is whether there was a competitive bidding process for the provision of EBKs. A competitive bidding process would have specified the technical, operational, and service requirements through a Request for Proposal (RFP). The City must account for its selection of Alphabet (Sidewalk/Intersection/CityBridge) as the sole provider of EBKs and explain why it did not release an RFP so that other companies could compete for part or all of the business. If the City states that no other companies possessed EBKs, then it must do the following:

- 1) provide dated due diligence that was conducted before the public hearing took place that concluded no other companies could provide units with the required functionality or could not provide the underlying communications network, and,
- 2) justify why it didn’t create an RFP so that potential competitors could develop proposals for supplying Wi-Fi units that could provide the service, advertising, communications network capabilities.

If the City says that there was not enough time for an RFP process, it must explain why it was so urgent to deploy the units now and not in the future when more companies could be manufacturing them and thus competitive bids could be taken.

The fact is, there was no urgency to deploy free wireless Wi-Fi service, and therefore no justification for waiving an RFP process that would include multiple vendors. There really are no critical reasons that could justify an urgency claim by the City since the provision of a free broadband, non-utility Wi-Fi service is simply not urgent. The vast majority of people have cell phones - both rich and poor – so there is no urgency for providing voice communications. Those at the lowest rungs of the economic ladder can receive free cell phones and service from the Federal government. Moreover, pay phones are located throughout the city and affordable to all. So, the City would need to prove that there was an urgency in providing a non-utility, discretionary consumer communications service if it used this as the rationale for not taking competitive bids.

Federal and State Authorities Should Investigate Possible Ethics and Legal Violations in the Awarding of the EBK Wi-Fi Monopoly to Alphabet (Sidewalk/Intersection/CityBridge) by the City of New York

A company called CityBridge was awarded the initial franchise to provide free Wi-Fi broadband service in New York City as well as to serve electronic advertisements through Electronic Billboard Kiosks (EBKs). The company was later acquired by Alphabet/Sidewalk/Intersection. Three executive employees of Sidewalk/Intersection were high level employees of the City of New York who may have had influence or control over the process to: 1) make a positive determination to deploy a monopoly franchise to provide free Wi-Fi service in New York City and 2) award the monopoly franchise to the company in which they would later be employed.

The Stop LinkNYC Primer

The three Sidewalk/Intersection employees are:

Daniel Doctoroff, Chief Executive Officer. He is a former NYC Deputy Mayor of Economic Development.
Joshua Sireman, Chief Development Officer. He is a former Chief of Staff to the NYC Deputy Mayor of Economic Development.
Rohit Aggarwala, Chief Policy Officer. He is a former NYC Director of the Office of Long-term Planning and Sustainability.

The New York Times reported in a March 16, 2016 article that Sidewalk/Intersection was created in June 2015 and conceived by Mr. Doctoroff:

“Sidewalk was hatched out of Google last June (June 2015) as an independent company that will use technology to solve urban problems — yet another example of how the Internet giant has strayed far and wide from its initial mission in online search. The company is based in New York and was conceived by Mr. Doctoroff, along with a team of Google employees led by Larry Page, one of Google’s founders and now Alphabet’s chief executive.”

There are a number of questions and issues that should be looked at with respect to the awarding of the franchise to a company whose CEO is the former Deputy Mayor of Economic Development, and who has two other former high ranking New York City employees working for him who may have been involved in the franchise process.

One area to look at is the timeline of when the idea was created and when it was first worked on by Mr. Doctoroff (and perhaps Mr. Aggarwala and Mr. Sireman). Specifically, did he conceive of or work on the idea as an employee of the City of New York.

Federal and State legal authorities should consider how a complex technology product and communications network could be “hatched” in June 2015 and then brought to market in less than one year, since the EBK network began beta test deployment in Q1/2016. This timeline does not comport with any type of reality with respect to the time it takes to bring a large, manufactured technology product (the EBK) and complex communications network (the Wi-Fi infrastructure) to market. It takes a lot more time than 6 to 8 months to create, design, test, and deploy a technology product and network infrastructure (in the beta test) as complex as the EBK Wi-Fi network (from June 2015 when Doctoroff claims he created the idea to Q1 2016 when the EBKs began deployment).

It stretches credulity that the life cycle to bring the EBK unit and the underlying communications network from concept to beta test was less than 9 months. This incredibly short time frame for conceiving, manufacturing, and deploying a complex technology product and network raises questions as to either the accuracy of the New York Times article or what it was told by Alphabet and/or Mr. Doctoroff. **This point is important because Alphabet maintains that this idea came about after Mr. Doctoroff left the City’s employment. The EBK network’s incredibly short timeline from concept to implementation raises the issue as to whether this idea was actually created and worked on by Mr. Doctoroff well before June 2015; that is, while he was employed by the City in his role as NYC Deputy Mayor of Economic Development. The same is true for Mr. Aggarwala and Mr. Sireman.**

The public should know whether Doctoroff, Aggarwala and Sireman worked on this idea in their high level capacities for the City. Areas that should be investigated by Federal and State legal authorities include:

- 1) Whether the justification for providing free wireless broadband service is actually true; that is, whether “over 25% of New Yorkers lack high-speed broadband service” (see previous section on this topic).
- 2) Whether Alphabet’s and the City’s justification of serving the “over 25%” population was a false justification to get the Wi-Fi monopoly franchise approved in order for Alphabet to compete directly against established wireless and wireline companies providing Internet and broadband service; and, to

The Stop LinkNYC Primer

compete against them with free Wi-Fi service funded by advertising fees, which it can charge by virtue of possessing a monopoly EBK Wi-Fi franchise given to it by the City of New York.

- 3) Whether there is a demonstrable need for free broadband Wi-Fi service throughout all of New York City – that would justify deployment of 10,000 EBKs - for the purpose of accessing broadband through mobile and home computing devices.
- 4) Whether the deployment strategy of the units is being done to serve the “over 25%” population. From the Franchise Agreement’s SRV Attachment Section 1.2.1, 52% (3,900) of the 7,500 LinkNYC EBKs that are required to be deployed are being installed in Manhattan, the wealthiest of the five boroughs. It does not pass the smell test that this deployment strategy is being done to serve the “over 25%” population that lacks high-speed broadband, which common sense would say are largely in the four other, less wealthy boroughs. Additionally, Manhattan has only 17% of New York City’s total population. Even if the remaining 2,500 units were to be deployed only in the other four boroughs, it still does not pass the smell test that they would cover the target population since they would comprise only 60% of the 10,000 units.
- 5) Whether Doctoroff, Aggarwala or Sireman worked on the idea of a free Wi-Fi network supported by advertising revenue during working hours when employed by the City. If they did, were protocols and legal processes followed with respect to government officials working on private business plans – or with private companies - from which they would derive a future, personal financial benefit due to the City’s awarding of a monopoly franchise to a company that they either were or became senior executives.
- 6) Whether: 1) the approval of the EBKs by the City, and 2) the awarding of the monopoly franchise to Sidewalk/Intersection/CityBridge was biased or prejudiced because of Doctoroff’s, Arrgawal’s, and Shireman’s (then) current or former employment as high ranking NYC employees, which may have given them influence or control over departments involved in granting the franchise.
- 7) The propriety, ethics, and legality of allowing former high-ranking City officials (Doctoroff, Aggarwala, or Sireman) to be employed as senior executives in a company that was granted a monopoly to provide Wi-Fi services to the City, where they likely will earn sizeable compensation through base salary, bonuses, and stock options.
- 8) The propriety, ethics, and legality of allowing former high-ranking City officials (Doctoroff, Aggarwala, or Sireman) to be employed by a City franchise that required the approval by departments over which they may have had managerial control or non-managerial operational and/or organizational influence .
- 9) Whether, due to the professional (and perhaps personal) relationship between Mr. Doctoroff and former Mayor Michael Bloomberg, the two worked together while City employees to lay the groundwork for granting a Wi-Fi monopoly to a company of which Mr. Doctoroff would later become CEO. Was there intent on both their parts to get the franchise approved so that Mr. Doctoroff could become its CEO at a future date? After his employment with the City was terminated, Mr. Doctoroff became CEO of Bloomberg Corporation, which was founded by former NYC Mayor Michael Bloomberg and to whom Mr. Doctoroff reported while serving as a Deputy Mayor of NYC. Mr. Doctoroff was also an employee of Bloomberg Corporation prior to his employment with the City. After ending his role as CEO of Bloomberg Corporation, Mr. Doctoroff became CEO of Sidewalk/Intersection, and Mr. Bloomberg became (again) CEO of Bloomberg Corporation.
- 10) Whether, after their terminations as City employees, Doctoroff, Aggarwala, and Sireman had meetings or conversations with other City employees, including Mayors Michael Bloomberg and Bill de Blasio, which did not conform to legal protocol and process for former government employees or high-ranking employees seeking to do business with the City.

The Stop LinkNYC Primer

- 11) Whether Doctoroff's, Aggarwala's and Sireman's relationships with City departments or with employees who reported to them or over whom they had non-management operational or organizational influence contributed to: a) approval of the EBK project by the City, and b) the City's decision not to consider competing alternatives to Alphabet's (Sidewalk/Intersection) offering.
- 12) Whether Doctoroff and/or Aggarwala and/or Sireman worked together to: a) create a false case for needing free Wi-Fi broadband service in New York City, b) worked with each other and other City employees to approve a monopoly franchise for providing such service, c) worked with each other and other City employees to award the monopoly contract to CityBridge (Alphabet/Sidewalk/Intersection) and d) engaged Alphabet/Sidewalk/Intersection/CityBridge employees in discussions to hire them in senior level positions as a quid pro quo for influencing the City to grant the company the monopoly franchise. (CityBridge is the initial company that was awarded the Wi-Fi monopoly franchise and was acquired by Sidewalk/Intersection).
- 13) Whether Doctoroff, Aggarwala, and Sireman recruited and hired any individuals from the City of New York who were involved in the evaluation and approval of the monopoly franchise. This includes, but is not limited to, individuals in the Department of Information Technology, Department of Transportation, the Franchise Concession and Review Committee, the Corporation Counsel, the Department of Economic Development, and the Office of Long-term Planning and Sustainability. Hires from these and other City departments after the franchise was awarded to CityBridge (Alphabet/Sidewalk/Intersection) may indicate a quid pro quo to support and approve the franchise to the company of which they are senior executives.
- 14) Whether Doctoroff, Aggarwala, or Sireman, in their capacities as Sidewalk/Intersection employees, have provided business opportunities to contractors the City might have hired for the evaluation and awarding of the Wi-Fi franchise. Business opportunities provided to these contractors while employed by Sidewalk/Intersection may indicate a quid pro quo. That is to say, the quid pro quo would be that promises were made by Doctoroff, Aggarwala, or Sireman – as City of New York employees - to have Sidewalk/Intersection give future business opportunities to contractors who made favorable recommendations in both the evaluation and awarding processes for the Wi-Fi monopoly franchise.
- 15) Whether Doctoroff, Aggarwala, Sireman, Michael Bloomberg, Bill de Blasio, and other City employees worked to get the free Wi-Fi monopoly approved in order to harm or even decimate the competitive market for wireless and wireline broadband services, the result of which would have future financial benefits to the City – due to its variable revenue agreement with Alphabet – as well as to those City employees who later would become employees of the franchise company, Sidewalk/Intersection.
- 16) Whether Mr. Doctoroff's former company and Michael Bloomberg's current company, Bloomberg Corporation, is receiving a benefit from the EBK Wi-Fi network that enables it to either increase its revenues, lower its operating and/or capital costs, or both. Since Bloomberg Corporation's headquarters is in Manhattan, there might have been an incentive for Doctoroff and Bloomberg – as Deputy Mayor and Mayor, respectively - to champion the Wi-Fi network in order to further the financial interests of the company of which they were former and current CEOs. An example of a financial benefit to Bloomberg Corporation would be the ability to lower its operating costs for Internet service by using free EBK Wi-Fi in conjunction with Virtual Private Networking (VPN) for internal corporation communications. This would allow the company to reduce or forgo purchasing fee-for-service Internet access from an existing wireline or wireless vendor. The company could also use the free EBK Wi-Fi service as its communications network with respect to its main line of business, which is to provide financial market information and data to financial services organizations throughout the world. By utilizing the free Wi-Fi service, it might be able to significantly reduce the communications costs associated with delivering its information services to its customers.

Conclusions and Recommendations

The LinkNYC EBK Wi-Fi and Advertising network needs to be **removed** – in its entirety – from all of New York City for the following reasons:

- 1) The negative quality of life created by the EBK form factor and from displaying electronic advertising on the Wi-Fi units throughout New York City’s residential and mixed residential/commercial areas.
- 2) The issues pertaining to privacy, tracking, surveillance, and Constitutional rights.
- 3) The potential health issues from RF radiation emitting from the EBK units.
- 4) The potential use of the EBKs for transportation-related projects, which was not part of the justification for the Wi-Fi franchise.
- 5) The financial harm and viability to wireline, wireless, and Web service companies due to the provision of free broadband Wi-Fi service by the monopoly public-private partnership.
- 6) The illegal video, audio, audio sensing, and photographic capabilities included in the EBK units.

Federal and State legal and regulatory authorities need to conduct an investigation into:

- 1) The claim that “over 25% of New Yorkers lack high-speed broadband service”. In addition, why 52% of the EBK Wi-Fi units are being deployed in Manhattan, the wealthiest of the five boroughs of New York City, when it has proportionally less than the “over 25%” population compared to the other boroughs and comprises only 7% of the land area of the five boroughs collectively.
- 2) The potential ethics and legal violations by former City of New York employees, including those who became senior executives of Sidewalk/Intersection.
- 3) The anti-competitive, monopolistic nature of the LinkNYC EBK Wi-Fi service, including how device metadata collected from the EBK Wi-Fi units can be used by Alphabet to give it an unfair competitive advantage in its other Web services businesses.

Note to Federal and State Attorneys General and Regulatory Agencies

In addition to evaluating the issues raised in this document that fall under your authorities, it is important to consider the City of New York’s approval of the LinkNYC Wi-Fi and Advertising Network as a classic “bait-and-switch” scheme. That is to say, that the City of New York created and presented a false or tenuous case – in conjunction with Alphabet/Sidewalk/Intersection/CityBridge - for the need of a free public Wi-Fi network to serve, as they claim, the “over 25% of New Yorkers who lack high-speed broadband service for the purpose of closing the digital divide” in order:

- 1) to generate significant amounts of revenue for the City through a variable revenue generation model based on digital advertising and fee-for-service offerings through the LinkNYC EBKs, where the City reaps a majority of the revenue – over 50% – for the life of its monopoly Wi-Fi & Advertising franchise contract with Alphabet,
- 2) to harm and/or decimate the competitive marketplace for high-speed broadband Internet service by providing a free, Internet access alternative to fee-for-service Internet access offerings provided by wireline and wireless service companies - which it is able to do solely because of its ownership of the city’s sidewalks - in order to increase the revenue it receives under the contract through the LinkNYC EBK network’s fee-for-service offerings, and
- 3) to install a massive surveillance network to monitor, locate, and track people – via mobile device MAC Addresses, vehicle license plates, and facial/picture recognition – throughout New York City and in particular in Manhattan, down to any specific block with its required deployment of 3,900 LinkNYC EBKs which will blanket this borough.

Appendix 1

**Alphabet/Sidewalk’s Map of 7,500 LinkNYC Electronic Billboard Wi-Fi Kiosks in NYC
(Another 2,500 units may be deployed, increasing the “dot density” in NYC by 33%)**

