# NYC INTERNET *REMASTERED*

## A Privacy & Equity Analysis of the New York City Internet Master Plan

**ALBERT FOX CAHN, ESQ.**
**CAROLINE MAGEE**

**DECEMBER 21, 2021**

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

Supported in part by a grant from the Open Society Foundations and by the John D. and Catherine T. MacArthur Foundation

## EXECUTIVE SUMMARY

On January 7, 2020, New York City released its Internet Master Plan. The document identified how many New Yorkers lacked access to broadband and what the City intended to do about it. The numbers were staggering: 46% of New York households in poverty lack a home broadband subscription.[1]

But what had been a problem evolved into a crisis when the COVID-19 pandemic descended on New York City in March. For the first time, New Yorkers had to stay home: as New York's 1.1 million public school students logged into Zoom for the first time, and their parents tried to take phone meetings in the same rooms, it became clear that the internet, once a luxury, was now a necessity.

As the fall semester loomed, the de Blasio administration tried to close the gap in July 2020, investing $157 million for providing low-or-no-cost internet to 600,000 New Yorkers, one-third of whom live in New York City Housing Authority housing.[2] The City is scrambling. In this light, a plan to expand internet access for residents of New York City is much needed and reflects the modern reality of reliable, affordable internet access as a barrier for reaching public services and economic opportunities. What is missing from the City's Internet Master Plan, however, is a needed degree of specificity on the privacy and cybersecurity protections built into this planned internet expansion.

This document therefore details:

- what technologies the plan suggests for expanding New Yorkers' access;
- the security risks associated with those technologies;
- what privacy protections are conferred to New Yorkers by existing legislation;
- what little the Internet Master Plan actually does say about privacy; and
- the impact on low-income New Yorkers.

[1] New York City Mayors Office of the Chief Technology Officer, "The New York City Internet Master Plan," 11, January 2020, https://www1.nyc.gov/assets/cto/downloads/internet-master-plan/NYC_IMP_1.7.20_FINAL-2.pdf.
[2] Kristine Garcia, "NYC Invests $157 Million to Provide High-Speed Internet for Low-Income Communities," *PIX 11*, July 7, 2020, https://pix11.com/news/local-news/nyc-invests-157-million-to-provide-high-speed-internet-for-low-income-communities/; Peter Szekeley, "New York City to Seek Assessment on Internet Providers to Fund Low-Income Service," *Reuters*, July 7, 2020, https://www.reuters.com/article/us-new-york-internet/new-york-city-to-seek-assessment-on-internet-providers-to-fund-low-income-service-idUSKBN2482NA. The City also seemingly re-announced this program just a few days ago. Matt Troutman, "NYC Invests In 5G: $157M Going Toward Expanded Internet Access," *Patch*, March 3, 2021, https://patch.com/new-york/new-york-city/nyc-invests-5g-157m-going-toward-expanded-internet-access; *Mayor Bill de Blasio Holds Media Availability*, 2021, https://youtu.be/mC0Iq-X-Dd8?t=321; New York City Mayor's Office of the Chief Technology Officer, "Twitter Post," March 1, 2021, https://twitter.com/NYC_CTO/status/1366551966181122050.

## I. Introduction

On January 7, 2020, New York City Mayor Bill de Blasio's administration released the "Internet Master Plan."[3] The 88-page document is ambitious, and identified, among the problems, that 29% of New Yorkers do not have a home broadband subscription, and laid out ways to remedy this gap; that number jumps to a staggering 46% when limited to a count of individuals living in poverty.[4] The document wasn't offered as the City's concrete plan, but as a "roadmap to a future-ready city."

And then COVID-19 happened.

In March 2020, life moved online. 1.1 million New York City schoolchildren were sent home for the remainder of the semester.[5] All but essential workers were ordered to stay home.[6] Offices, restaurants, bars, and music venues closed.[7] Access to the internet went from being something everyone in a "future-ready city" needed to something that all 8.3 million residents of New York City quite literally needed to attend school, do their jobs, apply for unemployment, and access public health information about the pandemic.[8] If 29% of all New Yorkers without a home broadband subscription hadn't seemed like a crisis before, it had certainly become one now.

In July, the City took steps to close the gap. $157 million was dedicated to offer internet service options to 600,000 New Yorkers, a third of whom live in New York City Housing Authority (NYCHA) residences.[9] "The COVID-19 pandemic shows that staying healthy depends on staying connected," Dr. Raul Perea-Henze, Deputy Mayor for Health and Human Services and co-chair of the Taskforce on Racial Inclusion and Equity, acknowledged.[10]

But these dollars are poorly spent if the City does not ensure that data privacy is a priority. The City will face an uphill battle on that front: technology poses threats to New Yorkers, not just benefits.[11] Beyond New York City, in fact, there is growing national concern about the impact of technology. In a November 2019 Pew poll, 63% of Americans admitted to thinking "it is not possible to go

---

[3] "De Blasio Administration Releases Internet Master Plan For City's Broadband Future," *NYC.gov* (press release), January 7, 2020, https://www1.nyc.gov/office-of-the-mayor/news/010-20/de-blasio-administration-releases-internet-master-plan-city-s-broadband-future.

[4] "The New York City Internet Master Plan," ii.

[5] Eliza Shapiro, "New York City Public Schools to Close to Slow Spread of Coronavirus," *New York Times*, March 15, 2020, https://www.nytimes.com/2020/03/15/nyregion/nyc-schools-closed.html.

[6] Zack Fink and Zach Cuza, "Cuomo Orders Non-Essential Workers to Stay Home as Coronavirus Cases Soar Over 7,000," *New York 1*, March 21, 2020, https://www.ny1.com/nyc/all-boroughs/news/2020/03/20/new-york-nail-salons-and-barber-shops-ordered-to-close-during-coronavirus-outbreak.

[7] Victoria Merlino and David Brand, "New York Closes Bars and Restaurants to Stop Spread of COVID-19," *Queens Daily Eagle*, March 16, 2020, https://queenseagle.com/all/new-york-closes-bars-and-restaurants.

[8] United States Census, "Quick Facts," last visited December 14, 2021, https://www.census.gov/quickfacts/newyorkcitynewyork.

[9] "Mayor de Blasio and Taskforce on Racial Inclusion and Equity Announce Accelerated Internet Master Plan to Support Communities Hardest-Hit by COVID-19," *NYC.gov* (press release), July 7, 2020, https://www1.nyc.gov/office-of-the-mayor/news/499-20/mayor-de-blasio-taskforce-racial-inclusion-equity-accelerated-internet-master.

[10] *Id.*

[11] Angel Diaz, "New York City Police Department Surveillance Technology," *Brennan Center For Justice*, October 4, 2019, https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

through daily life without the government collecting data about them."[12] Even more – 84% – feel they have little or no control over the data that the government is collecting.[13]

To implement the Internet Master Plan most meaningfully, the City needs to regain New Yorkers' trust. Providing access to the internet to all is more important than ever, but doing so at the expense of the privacy and peace of mind of New Yorkers will only undermine the ever-waning public trust in the government at a time when maintaining faith in City leadership is crucial for public health efforts. It is only by protecting New Yorkers' privacy that City Hall can most effectively close the digital divide and extend to all New Yorkers the kind of access to the internet they deserve.

## II. Background

There are many technologies available to the City, which the plan explores for bringing access to the internet to New Yorkers at home. Broadly speaking, broadband comes in three forms: wired, fixed wireless, and mobile wireless.[14] These different types of broadband each have their own requirements for "real estate," meaning where they go and how much space they take up.

Wired access consists of fairly well-known forms of access to the internet: fiber optics, DSL ("digital subscriber line"), and cable.[15] Fixed wireless access comes in less-familiar formats to the layperson: mmWave-FWA, free-space optics, and mesh.[16] And finally, mobile wireless access includes licensed 4G, LTE, and 5G cellular spectrum services, as well as unlicensed, low-power Wi-Fi hotspots.[17]

To dissect the above a little: DSL and cable run on existing infrastructure – internet access via DSL relies on phone lines, and cabled internet access relies on cable lines.[18] Because these phone and cable lines are already laid, they are convenient for companies to use to provide internet connectivity. That said, they have speed issues. DSL has significantly slower speeds when uploading data rather than downloading, so it would be fine for reading an article but would slow significantly when uploading a video to YouTube; cable speeds slow as more neighborhood users sign on to the same connection, like during work hours when everyone is working from home.[19] Expanding this infrastructure is probably a poor place to look to make the city "future ready," but it at least serves a purpose if the City is triaging the digital divide (focusing on getting broadband into residences faster rather than building out the infrastructure). The third type of access under the "wired access" umbrella is fiber optics. On the one hand, fiber optics avoid the speed problems of DSL and cable not because it has infinite bandwidth but because it has significantly more than either of the other two. On the other hand, it's problematic on the infrastructure front: fiber hasn't been laid in every neighborhood and is expensive to lay.

---

[12] Brooke Auxier, et. al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center*, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[13] *Id.*
[14] "The New York City Internet Master Plan."
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Best Buy, "Cable vs. DSL," *Bestbuy.com* (blog), last visited December 14, 2021, https://www.bestbuy.com/site/tech-tips/compare-cable-dsl/pcmcat748301881084.c?id=pcmcat748301881084.
[19] *Id.*

In fact, the expense of laying fiber is a significant consideration for the "fixed wireless" solutions too. Whereas the "wired access" internet access would push fiber directly into residences, "fixed wireless" internet access depends on a fiber-connected building broadcasting the internet out. In other words, in the former case, city residents would have a physical wire running directly into their homes, while in the latter case, city residents could connect to a building in the area that is linked directly to the wiring. This latter "fixed wireless" approach works best from a tall building down to a neighborhood of lower/varying building heights, and would thus be a better solution for New York City's outer boroughs than much of Manhattan.[20] An example of this kind of technology that is gaining traction is mesh[21], which made news during the Occupy City Hall protests in June and July 2020 by providing free public Wi-Fi for protesters through a hub the group NYC Mesh had installed at Manhattan Borough President Gale Brewer's office.[22] Of the "fixed wireless" solutions, mesh is the only realistic one (and one already in use by "regular" consumers): free space optics is only just leaving the lab for consideration of real-world use[23], and mmWave-FWA is, as the Internet Master Plan notes, "highly susceptible to interference."[24]

In much of the United States, internet service delivery is primarily regulated through the Federal Communications Commission; however, New York City holds unique authority to regulate how the internet is delivered. In Manhattan and the Bronx, conduits (the underground space in which fiber is laid) are owned by the company Empire City Subway ("ECS"), a subsidiary of Verizon. While a turn-of-the-20th-century era deal with the City demands that third parties have access to it, an audit of ECS by then-City Comptroller John Liu revealed that, in 2007-2008, only 1.3% of the newly constructed conduits were in use by an entity other than Verizon.[25] The City must enforce its own agreement – now more than a century old – because the alternative is very expensive, so much so that it disincentivizes such building in areas touched by ECS. Complicating matters is that the expense varies from neighborhood to neighborhood: in Long Island City, it can be more than 25 times as expensive to lay the same distance as it would be through ECS in Manhattan or the Bronx.[26]

Fiber can be aboveground (sometimes called "aerial" fiber) as opposed to in these overpriced conduits, but is then susceptible to everything that comes with being outside: high winds, hail, freezing rain, etc. This was evidenced in the City's post-mortem analysis of infrastructure's ability to withstand Superstorm Sandy, "A Stronger, More Resilient New York": new coaxial and fiber optic

[20] "The New York City Internet Master Plan."
[21] "Most NYC Mesh community members ('nodes') have wireless routers mounted on a rooftop or balcony to connect to other nodes, forming a network. Our network in turn peers (connects) with many other networks at an Internet exchange point (IXP), providing direct access to the Internet without the intermediary of a commercial Internet Service Provider. NYC Mesh maintains a number of primary Internet exchange points that we call 'Supernodes.'" "Frequently Asked Questions," *NYC Mesh* (blog), last visited December 14, 2021, https://www.nycmesh.net/faq/#how.
[22] Rob, "Occupy City Hall WiFi," *NYC Mesh* (blog), July 1, 2020, https://www.nycmesh.net/blog/occupy-city-hall/.
[23] Andrew Williams, "Free-Space Optics Beginning to Achieve Real-World Value," *International Society for Optics and Photonics* (blog), February 13, 2020, https://spie.org/news/free-space-optics-beginning-to-achieve-real-world-value?SSO=1.
[24] "The New York City Internet Master Plan," 42.
[25] City of New York Office of the Comptroller, "Audit on the Payment by Empire City Subway of License Fees Due the City and Compliance with Certain Provisions of its License Agreement," June 2, 2010, https://comptroller.nyc.gov/wp-content/uploads/documents/FP08_103A.pdf; Susan Crawford, "I'm Suing New York City to Loosen Verizon's Iron Grip," June 21, 2017, https://www.wired.com/story/im-suing-new-york-city-to-loosen-verizons-iron-grip/.
[26] Matthew Flamm, "Race Is on to Bring Broadband to New Yorkers," June 18, 2019, https://www.crainsnewyork.com/features/race-bring-broadband-outer-boroughs.

cable survived the storm better than did copper cable, though in the outer boroughs there was some disruption due to downed trees and high winds.[27]

## III. Privacy

### *a. Infrastructure of the internet and the associated security risks*

The expense and durability of fiber aside, it isn't perfectly secure. This can be assessed along two veins: physical security risks and cybersecurity risks.

Regarding physical security risks: if a bad actor can gain physical access to the fiber, such as by placing a tap on a fiber line, that actor can access the packets being sent (packets being the chunks of data tagged with a source and destination that your computer receives and sends that, together, comprise the internet).[28] This is more easily avoided when the fiber is underground – it is inherently more of an ordeal to access it – but by no means does that eliminate the risk. In a world where "every New York City household [was connected] with fiber-optic service and include[d] fixed wireless service where possible, along with basic mobile wireless coverage throughout city streets," the Internet Master Plan cites the need for 24,000 poles or street furniture, 800 rooftops, and additional infrastructure. With that big of a real estate commitment, the internet is only as secure as those spots are. These spaces are not immune to threats like USB drives, infected with malicious software and server room break-ins with rogue device installations to intercept data.[29]

The cybersecurity risks to internet fiber look different, but they follow the same idea of an unauthorized user gaining access to data. This is more like unauthorized data access through piggybacking, or evil twin attacks, among other threats.[30] These threats aren't unique to fiber and exist however one accesses the internet.

New Yorkers face two discrete threats: hackers and criminals who want to break into our networks and computers and government agencies that are legally entitled to do so. The latter occurs at exchange points and internet service provider facilities by the federal government, and then there is the matter of municipal collection.

To make the mechanics of this clear: internet exchange points are "a physical location where different IP networks meet to exchange traffic with each other with copper or fiber cables interconnecting their equipment, usually via one or more Ethernet switches."[31] Internationally, there

[27] The City of New York Mayor Michael Bloomberg, "A Stronger, More Resilient, New York," June 2013, https://www1.nyc.gov/assets/sirr/downloads/pdf/Ch_9_Telecommunications_FINAL_singles.pdf.
[28] "What Are the Issues Surrounding Fiber Optics," *George Mason University* (blog), last visited December 14, 2021, http://mason.gmu.edu/~jharri35/content3.html.
[29] "Physical and Cybersecurity Defense: How Hybrid Attacks Are Raising the Stakes," *Resolver* (blog), September 27, 2021, https://www.resolver.com/blog/physical-and-cybersecurity-defense-hybrid-attacks/.
[30] "Security Tip (ST05-003): Securing Wireless Networks," *CISA.gov* (blog), May 8, 2020, https://www.cisa.gov/uscert/ncas/tips/ST05-003.
[31] Internet Society, "The Internet Exchange Point Toolkit & Best Practices Guide," February 2014, https://www.ixptoolkit.org/wp-content/uploads/2016/08/Global-IXPToolkit_Collaborative-Draft_Feb-24.pdf.

has been a growing problem with government surveillance at these sites.[32] These switches – and the potential for surveillance at them – was partially the subject of the testimony of Edward Snowden, who told members of the European Parliament that the NSA was encouraging this kind of collection and then demanding the data themselves.[33]

Similarly, the American federal government carries out this kind of surveillance with internet service providers. The National Security Agency ("NSA") was revealed to be engaging in exactly this kind of surveillance of AT&T customers (working in partnership with AT&T) in documents released by Edward Snowden.[34] The Intercept has identified AT&T buildings in eight American cities (including New York City) that are "central to an NSA spying initiative that has for years monitored billions of emails, phone calls, and online chats passing across U.S. territory."[35]

If this unbelievable intrusion into communications on American soil by the American government wasn't terrifying enough, AT&T is not only allowing this: the NSA referred to the company's "extreme willingness to help."[36]

This is different from fears of municipal collection by private actors, which may happen as a result of public-private partnerships. Such deals may bargain away users' right to privacy for free or low-cost access through shortsighted decisions by the municipality. The private entities may then be entitled to collect data about you.

Municipal collection makes it clear that the federal government isn't the only thing to fear. The Internet Master Plan talks about strengthening "public Wi-Fi networks with Quad9 DNS-based cybersecurity."[37] This sounds like a solution, but looking more deeply at both Quad9 and even the global-level DNS makes it clear it isn't. To understand why, a little bit of background: Quad9 is a recursive resolver, or ½ of user's engagement with the DNS; the "first stop" in a DNS query that will ultimately take you to a website.[38] Quad9 claims they are not retaining specific IP addresses and what aggregated data they do retain is formatted in such a way that is impossible to reverse engineer identities out of that data.[39] There are two problems, then, with Quad9. First, the claim that data

[32] Monika Ermert, "Largest Internet Exchange Point Announces Complaint Against Snooping," *Intellectual Property Watch*, April 24, 2015, http://www.ip-watch.org/2015/04/24/largest-internet-exchange-point-announces-complaint-against-snooping/; David Meyer, "German Intelligence Can No Longer Freely Spy on the World's Internet Traffic, Top Court Rules," *Fortune*, May 19, 2020, https://fortune.com/2020/05/19/germany-snowden-spying-bnd-nsa-de-cix/.
[33] Statement of Edward Snowden before the European Parliament, https://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.
[34] Julia Anguin, et. al., "AT&T Helped U.S. Spy on Internet on a Vast Scale," *New York Times*, August 15, 2015, https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.
[35] Ryan Gallagher and Henrik Moltke, "The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities," *The Intercept*, June 25, 2018, https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.
[36] *Id.*
[37] "The New York City Internet Master Plan," 32.
[38] DNS Server Types, Learning Center, DNS Glossary, CloudFlare, accessed December 14, 2021, https://www.cloudflare.com/learning/dns/dns-server-types/#:~:text=What%20is%20a%20DNS%20recursive,client%20and%20a%20DNS%20nameserver.
[39] "Data and Privacy Policy," Service, Privacy, Quad9, accessed December 14, 2021, https://www.quad9.net/policy/.

cannot be "re-identified" is largely wrong.[40] With enough time and money, there is very little data that cannot be re-identified.

Second: Quad9's data storage and privacy claims aside, this recursive resolver was developed by a nonprofit founded and funded by the Manhattan County District Attorney's Office and law enforcement partners.[41] This should terrify New Yorkers. The obvious vulnerability is overstepping by law enforcement – in particular by the Manhattan District Attorney's Office, which is already more punitive of poor New Yorkers than rich,[42] accused of hiding evidence,[43] and has claimed phone encryption "creates serious new risks" for New Yorkers.[44] It is all too easy to imagine a case where, after claiming the data is not collected, the DA's office re-identifies data, or a flaw in the supposedly privacy-minded data storage is revealed, and data has been collected, and the DA's office uses it.

The reality of DNS is that it is fundamentally vulnerable at the global level *because of how it was designed*. It was built this way. DNS queries and responses are largely sent in cleartext, and are thus susceptible to anyone with the appropriate skillset looking to listen.[45] There are efforts by browsers to implement DNS over HTTPS, as well as work on standards, but unfortunately, this eludes the fundamental fact that the architecture of DNS was not created with privacy in mind. Understanding this reality sheds some light on why the City can only do so much.

Given the risks inherent in Quad9, the architecture of DNS, and that the government *was* in fact spying on the communications of so many Americans through AT&T, it is hardly any wonder that 84% of Americans feel like they have no or little control over what data the government collects on them.[46] As previously stated, the City alone cannot fix systemic problems with the internet, nor can it delivery a privacy-perfect internet to residents. But expanding broadband access can mean creating a yet-more-granular way to track New Yorkers, and there are dozens of choices the City can make to mitigate those risks and better educate New Yorkers on the City's decisions. The City should invest in genuine public education efforts—as opposed to the great bait-and-switch of internet privacy

---

[40] Natasha Lomas, "Researchers Spotlight the Lie of 'Anonymous' Data," *TechCrunch*, July 24, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/; Boris Lubarsky, "Re-Identification of 'Anonymized' Data," *Georgetown Law Technology Review* 202, no. 1 (April 2017) https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

[41] "Quad9 Enabled Across New York City Guest and Public WiFi," *Quad9*, March 28, 2018, https://www.quad9.net/quad9-enabled-across-new-york-city-guest-and-public-wifi/.

[42] Tom Robbins, "The People vs. Cy Vance," *The Marshall Project*, April 29, 2018, https://www.themarshallproject.org/2018/04/29/the-people-vs-cy-vance.

[43] Greg B. Smith, "A Top Prosecutor in Manhattan DA Vance's Office Accused of Hiding Evidence," *The City*, January 23, 2020, https://www.thecity.nyc/2020/1/23/21210564/a-top-prosecutor-in-manhattan-da-vance-s-office-accused-of-hiding-evidence.

[44] Colby Hamilton, "Vance Says Phone Encryption Hurts Crime Victims," *Politico*, July 8, 2015, https://www.politico.com/states/new-york/city-hall/story/2015/07/vance-says-phone-encryption-hurts-crime-victims-023596.

[45] Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar, Jordan Holland, Austin Hounsel, and Paul Schmitt, "How DNS Over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem," *TPRC47: The 47th Research Conference on Communication, Information, and Internet Policy 2019* (July 27, 2019), https://www.cs.princeton.edu/~ahounsel/publications/tprc19.pdf.

[46] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center*, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/.

where education is merely a false offering. The City should also regularly and thoroughly disclose its data collection and use policies and practices, as well as communicate to New Yorkers how these fit within state and local laws restricting data collection and use. Moving forward, the Council or designated agencies will need to make specific transparency demands of the private entities involved in this plan, create penalties for ignoring them, and establish an absolute firewall between law enforcement entities and this data. The City has now declared what we already knew to be true: access to the internet is now a right, not a privilege. To honor that declaration and to get the buy-in the City both craves and requires, New York must not only make the internet more accessible, but do it right.

*b. Existing protections (state, federal) fall short of protecting New Yorkers*

New Yorkers will need new legal protections because what already exists falls short of offering the protection they deserve.

On the federal level, there's the Privacy Act of 1974. The Privacy Act of 1974 is not the only piece of privacy legislation on the federal level, but assuming the data at stake is neither health-related nor collected/retained by a financial institution, it is the most relevant one. This act theoretically protects US persons from the collection, use, and dissemination of data by federal agencies. However, as the Department of Justice's own treatise, published in 2015, indicates, "the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply."[47] It also doesn't even claim to protect US persons from state agencies, or from businesses.

On the state level, there is somehow even less protection. There is no state-level analog to the Privacy Act of 1974, and thus no protection against government entities collecting data on US persons. There is also no New York analog to the California Consumer Protection Act (the "CCPA"), and thus no protection against predatory businesses that constantly collect consumer data through digital devices and internet activity.[48] Instead, New York State frames data protection in the same light as the City does, not as protection from government misuse of data but as protection from rogue hackers. In 2019, in response to numerous data breaches, New York passed the SHIELD Act, which created requirements for businesses on appropriate safeguards for data.[49]

Additionally, there is legislation on the horizon: the New York Privacy Act,[50] a bill called a "CCPA clone with private right of action."[51] But even this legislation should establish a floor, not a ceiling, for New Yorkers' privacy. An example of how this bill must be only the first of many pieces of

[47] "Overview of the Privacy Act of 1974, 2015 Edition," Office of Privacy and Civil Liberties, U.S. Department of Justice, last modified February 25, 2021, https://www.justice.gov/opcl/file/793026/download.
[48] "California Consumer Privacy Act," Privacy, State of California Department of Justice Office of the Attorney General, accessed December 14, 2021, https://oag.ca.gov/privacy/ccpa (The CCPA establishes Californians' "right to know about the personal information a business collects about them and how it is used and shared; … right to delete personal information collected from them (with some exceptions); … right to opt-out of the sale of their personal information; and … right to non-discrimination for exercising their CCPA rights.").
[49] Francis J. Serbaroli, "The SHIELD Act: NY's New Data Protection Requirements Take Effect," *New York Law Journal*, November 25, 2019.
[50] "Senate Bill S567, 2021-2022 Legislative Session," New York State Senate, accessed December 14, 2021, https://www.nysenate.gov/legislation/bills/2021/S567.
[51] Kyle Fath and Melinda McLellan, "New York Legislature Introduces CCPA Clone with Private Right of Action," *JDSupra*, January 8, 2021, https://www.jdsupra.com/legalnews/new-york-legislature-introduces-ccpa-6501577/.

legislation to help protect New Yorkers: the fact that this bill does not require law enforcement to obtain a warrant before demanding data from vendors. Given how much information is collected by the internet, it is impossible to consider New Yorkers' data secure if the vendors collecting it can simply sell it to law enforcement. This will be an enormous problem for all New Yorkers, but will have a particular impact on undocumented New Yorkers given Immigration and Customs Enforcement's penchant for buying data it cannot simply collect itself.[52]

The City also promises it has improved its internal governance in recent years by creating the Mayor's Office of Information Privacy.[53] This office publishes quarterly reports on data breaches from within the City government. While this is important, it's important to put this enormous concession made by the government in perspective: this is the absolute least the City could do. These disclosures create a record of everything from ransomware attacks to technical errors to human mistakes that result in the improper sharing of data.[54] This isn't a bad thing. But it must only be the beginning.

New Yorkers need novel legislation that will prevent government access to data collected on them; this will prevent some of the more egregious harms practically guaranteed to occur when private actors are permitted to collect data on them. To earn New Yorkers' support in their plan to expand internet access, the City and the State must prove that they are serious about protecting New Yorkers from all sorts of threats – including themselves.

*c. The City's Plan to Protect Privacy*

The Internet Master Plan did offer some solutions to privacy; they were just incomplete and scattered, largely un-analytically, throughout the document. This occurred under the guise of making privacy a priority: the City, after all, included privacy in a list of the five core principles of the plan. A short list on a page titled "Digital Privacy" suggests that the City's approach is "holistic" and three-pronged, including administrative and legislative solutions, consumer education, and new technical tools. This short list is not the overwhelming show of force on privacy issues that New Yorkers deserve.

The first of these, "administrative and legislative solutions," is addressed earlier in this report. As concluded in that section, it does not provide enough protection for New Yorkers.

The second of the options is consumer education. Consumer education is the false flag of internet privacy and security because it is often paraded as a solution to privacy and security issues when it is actually a solution to liability, and to do it right requires enormous resource investment by the City. To put it another way: the problem is real; it's just that the solutions often offered don't solve it. There is a massive information asymmetry between businesses and consumers on data privacy and security, whether an individual trying to understand the cybersecurity provided by their bank or the average internet user trying to parse through a long, complex privacy policy to understand what data

[52] Rani Molla, "Law Enforcement Is Now Buying Cellphone Location Data From Marketers," *Vox*, February 7, 2020, https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration.
[53] "Welcome to the Mayor's Office of Information Privacy," NYC Mayor's Office of Information Privacy, accessed December 14, 2021, https://www1.nyc.gov/site/moip/index.page.
[54] "Quarterly Report of the Chief Privacy Officer on Agency Disclosures Made Under Exigent Circumstances or in Violation of the Identifying Information Law," NYC Mayor's Office of Information Privacy, December 29, 2020, https://www1.nyc.gov/assets/moip/downloads/pdf/CPO-Quarterly-Report-Q2-12-15-2020.pdf.

a website gathers on them.[55] The information asymmetry is not just in the access to information and the volume and quality of that information; it also lies in consumers not understanding the information they do have. In a Pew survey conducted in 2016, for example, only 1% of those polled answered 13 questions on cybersecurity correctly.[56] Only 11%, for example, correctly answered whether all traffic through a Wi-Fi router was automatically encrypted.[57] The City's thus-far proposed education solutions echo more hollowly in light of these statistics. The City has established a "Library Privacy Week" with various groups to raise "awareness" of the importance of online privacy,[58] but awareness is not enough. Instead, the City should push to develop specific guides about data collection occurring as part of or in relation to the Internet Master Plan, listing the names of every private entity involved at every level. Importantly, this guide could not be in so-called legalese: it would need to be written in easily understood language as well as in multiple languages.

Another solution often suggested for consumer education is more comprehensive privacy policies and terms of use, because these theoretically disclose to users what data is collected, how it is stored, how long it is retained, and how it will be used. But this is the aforementioned preferred way to actually avoid liability while creating the illusion of informed choices. They often are written deliberately in opaque language and legalese so as to confuse consumers.[59] By "informing" the consumer of the use of data, they remove liability on charges involving misuse.[60] Mary Stone Ross, the activist who led the movement to pass the CCPA, said of privacy policies that "they're clearly not written to inform a consumer. It's written to protect the interests of a business."[61]

A good example of this is one such policy already in place: the LinkNYC User Policy. LinkNYC kiosks are on many streets, providing "free" Wi-Fi for New Yorkers and visitors alike. As the oft-used phrase goes, if you're not paying for the product, you are the product. Users consent to the user policy – likely not reading it – and then, understandably, use the Wi-Fi. And LinkNYC promises to only collect anonymized, aggregated data – words that are used intentionally to create distance between the idea of user and data.[62] But the head of one of the companies behind LinkNYC himself said: "By having access to the browsing activity of people using the Wi-Fi — all anonymized and aggregated — we can actually then target ads to people in proximity and then obviously over time, track them through lots of different things, like beacons and location services, as well as their browsing activity. So in effect, what we're doing is replicating the digital experience in

---

[55] David Serabian, "Consumer Protection and Cybersecurity: The Consumer Education Gap," *Brookings Mountain West Publications* (2015): 1-16, https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1032&context=brookings_pubs.

[56] Kenneth Olmstead and Aaron Smith, "What the Public Knows About Cybersecurity," *Pew Research Center*, March 22, 2017, https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/.

[57] Olmstead and Smith, "What the Public Knows About Cybersecurity."

[58] "The New York City Internet Master Plan," 50; "Library Privacy Week," NYC Digital Safety: Privacy & Security, accessed December 14, 2021, https://libraryprivacyweek.nyc/.

[59] Kevin Litman-Navarro, "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," *New York Times*, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[60] Jocelyn Mackie, "Privacy Policies for Small Businesses," Terms Feed, last modified December 22, 2020, https://www.termsfeed.com/blog/privacy-policy-small-business/#Protection_From_Liability.

[61] Mary Stone Ross, "From the CIA to CCPA: What's Next in Privacy," May 2020 on BigIDeas On The Go, podcast, 4:30, https://open.spotify.com/episode/6x8cszs0GZjpIceiWn3X50#login.

[62] J.D. Biersdorfer, "Are the Free Wi-Fi Kiosks on New York Streets Safe?," *New York Times*, August 26, 2016, https://www.nytimes.com/2016/08/27/technology/personaltech/are-the-free-wi-fi-kiosks-on-new-york-streets-safe.html; Ava Kofman, "Are New York's Free Link NYC Internet Kiosks Tracking Your Movements?," *Intercept*, September 8, 2018, https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/.

physical space."[63] The use of "anonymized" and "target ads" in the same sentence belies the very lack of personalization he is claiming LinkNYC offers. It also suggests that these documents that inform the service-using public of data collection, use, and retention might be misleading.

Given that these privacy policies and terms of use are often difficult for above-college-level readers to meaningfully understand, they are not the answer to consumer education. Instead, to meaningfully claim to have educated consumers, the City must invest in actual consumer education. This will look like outreach to every community from trusted messengers, in multiple languages and geared at different age groups. This is why real consumer education is hard to do: there is no one-size-fits-all message, and that is precisely why privacy policies and terms of use do not work.

## IV. Equity

Wealth inequity is expanding in the United States,[64] and this is as true in looking at New York's broadband access as anywhere else. As noted, nearly half of New Yorkers living in poverty do not have broadband access at home.[65] When the Internet Master Plan was released, this clearly felt to the City like a long-term policy problem in need of a long-term solution; COVID-19 made it an emergency, and many questions remain about if and how the Internet Master Plan will address the glaring equity problems underpinning and exacerbated by internet accessibility.

Mayor de Blasio took steps in 2020 to do just that, throwing $157 million dollars behind an effort to bring low-or-no-cost internet access to 600,000 New Yorkers, one third of whom live in New York City Housing Authority housing.[66] These are good first steps but there will need to be more. The City should start by producing and publicly releasing an annual comparison of what City-provided internet access looks like (speed, bandwidth, cost) compared to that for people who can afford to independently pay for their own internet plans.

Last school year, New York City's 1.1 million public school students were largely online, only just recently returning to re-opening schools in March 2020.[67] Schools still close periodically, going remote for days or weeks as COVID-19 outbreaks sweep the student and teacher populations.[68] For months, New York City's students were simply at home, with whatever internet access they already possessed. For students with bad connections, this plan is already too little too late, to say nothing of everything that was online for adults well before the pandemic hit: job applications, bill payment, banking, housing applications.

This is ultimately the truth of the digital divide in New York City: it long predates the COVID-19 pandemic and will outlast it. This crisis just wrenched the people most affected by lack of internet away from the ways they had learned to cope: going to the library to use the internet

---

[63] Nick Pinto, "Google is Transforming NYC's Payphones into a 'Personalized Propaganda Engine,'" *Village Voice*, July 6, 2016, https://www.villagevoice.com/2016/07/06/google-is-transforming-nycs-payphones-into-a-personalized-propaganda-engine/.
[64] Bill Chappell, "U.S. Income Inequality Worsens, Widening to a New Gap," *NPR*, September 26, 2019, https://www.npr.org/2019/09/26/764654623/u-s-income-inequality-worsens-widening-to-a-new-gap.
[65] "The New York City Internet Master Plan," ii.
[66] "Mayor de Blasio and Taskforce on Racial Inclusion and Equity Announce Accelerated Internet Master Plan."
[67] "Mayor and Taskforce Announce Internet Master Plan."
[68] Mark Sundstrom, "Far Rockaway Middle School Closes Due to COVID Outbreak; 2nd Queens Closure This Week," *Pix 11*, November 11, 2021, https://pix11.com/news/coronavirus/queens-far-rockaway-middle-school-closed-covid-outbreak.

there, students staying late at school when they didn't have Wi-Fi at home, going to friends' houses. There have been endless articles about the inequities laid bare by COVID-19.[69] But the lack of affordable or any internet access to most New Yorkers must not be treated as a revelation but as symptomatic of a larger inequity in the city, and something that needs to be fixed as thoughtfully: with community input, with privacy protections, and with genuine investment in the future of New York City.

[69] Jay Caspian King, "Inequality Has Been Laid Bare by the Outbreak. Now What?," *New York Times Magazine*, May 20, 2020, https://www.nytimes.com/interactive/2020/05/20/magazine/covid-quarantine-inequality.html; Valerie Strauss, "How Covid-19 Has Laid Bare Vast Inequities in U.S. Public Education," *Washington Post*, April 14, 2020, https://www.washingtonpost.com/education/2020/04/14/how-covid-19-has-laid-bare-vast-inequities-us-public-education/.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT