# MUNICIPAL WI-FI AND THE THIRD-PARTY DOCTRINE: RETHINKING AN ANTIQUATED FRAMEWORK♦



## INTRODUCTION

On February 18, 2016, New York City Mayor Bill de Blasio announced LinkNYC, a plan to convert the City's "old payphones into Wi-Fi kiosks to create the world's largest and fastest free public Wi-Fi network."[1] The kiosks, called "Links," provide New Yorkers with a "Wi-Fi network with a 150-foot radius, free domestic calling, two USB charging ports, a tablet for accessing the internet, and a red 911 button



[1] Press Release, Office of the Mayor, Mayor de Blasio Announces Public Launch of LinkNYC Program, Largest and Fastest Free Municipal Wi-Fi Network in the World (Feb. 18, 2016) [hereinafter LinkNYC Launch], http://www1.nyc.gov/office-of-the-mayor/news/184-16/mayor-de-blasio-public-launch-LinkNYC-program-largest-fastest-free-municipal#/0.

to contact emergency services."[2] The kiosks were developed by CityBridge, a group of companies including Intersection, Qualcomm, and CIVIQ Smartscapes.[3] LinkNYC kiosks offer an encrypted network for HotSpot 2.0-enabled devices and "at least twenty-four hours of back-up battery power to enable 911 calling capability in the event of the loss of commercial power."[4]

LinkNYC is a joint undertaking between the City of New York and CityBridge, which will administer the services on behalf of the City.[5] The franchise agreement between the City and CityBridge authorizes "at least 7,500 Links – and as many as 10,000" across the five boroughs.[6]

LinkNYC is the latest in a slew of public Wi-Fi programs enacted by city planners in an attempt to bridge the so-called "digital divide."[7] The digital divide refers to the gap between those who have access to the Internet, broadband, or mobile phone service and those who do not.[8] Internet access is correlated with wealth, as wealthier Americans are more likely to have Internet access in their homes than poorer Americans.[9] Commentators have also noted that the digital divide tracks along racial lines in America.[10] "[H]undreds of cities now provide some form of online access,"[11] although bridging the gap between informational haves and have nots[12] has taken various forms.[13]

Public Wi-Fi programs have appeared around the nation, involving various levels of government action.[14] One approach is a purely public utility model, where government owned-and-operated, mostly city-wide "municipal broadband" networks are built and managed by cities

---

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *See* City of N.Y. Dep't of Info. Tech. & Telecomm., Franchise Agreement For the Installation, Operation, and Maintenance of Public Communications Structures in the Boroughs of the Bronx, Manhattan, Queens and Staten Island (2014) [hereinafter CityBridge Franchise Agreement], http://www1.nyc.gov/assets/doitt/downloads/pdf/Franchise-Agreement-for-Public-Communications-Structures-(REVISED-FINAL-12-10-2014).pdf.

[6] LinkNYC Launch, *supra* note 1.

[7] *See* Brooke Menschel, *One Web to Unite Us All: Bridging the Digital Divide*, 29 CARDOZO ARTS & ENT. L.J. 143, 149 (2011).

[8] *See id.* at 149–50.

[9] *See id.* at 140–50. As of 2011, "less than forty-seven percent of households earning a family income between $15,000 and $24,999 have Internet at home, while more than ninety-five percent of families earning more than $100,000 have Internet at home." *Id.* at 153 n.42.

[10] *See id.* at 152–54.

[11] *See* Enrique Armijo, *Kill Switches, Forum Doctrine, and the First Amendment's Digital Future*, 32 CARDOZO ARTS & ENT. L.J. 411, 425 (2014).

[12] *See* Menschel, *supra* note 7, at 149 (citation omitted).

[13] See Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1 (2007); *see also* Tim Gnatek, *Switchboard in the Sky*, N.Y. TIMES (May 3, 2006), http://www.nytimes.com/2006/05/03/technology/techspecial3/03utility.html.

[14] *See* Armijo, *supra* note 11, at 428, 429.

themselves.[15] These programs often use existing electricity infrastructure to run the programs.[16] Another approach is the increasingly common public-private partnership, such as LinkNYC, where a private Internet Service Provider (ISP) provides Internet access via Hotspot[17] in a particular public space "such as a neighborhood, business district, park, town hall, or transportation hub, thereby aggregating smaller service areas within their city limits, in cooperation with a municipality or its administrative subsidiary, at low or no cost to the user."[18] These projects are often undertaken for public purposes, ranging from education to economic development.[19] Commentators have observed that city officials hope that offering a municipal Wi-Fi service will encourage businesses to move to their community, attract visitors, and build a more vibrant city center. Additionally, wireless systems are increasingly being marketed to cities as a means to give more tools to "law enforcement, fire departments, and emergency services."[20] However, public-private partnerships raise important implications for public safety, free expression, and privacy rights.[21]

The LinkNYC program raises similar privacy concerns. Users must supply an email address before using the service to be informed of updates or changes to the service.[22] Each unit collects anonymous aggregated data to study for system use and diagnostics as well as to influence the large color advertising screens on the sides of the kiosk that subsidize the service.[23] However, consumer advocacy groups and the New York Civil Liberties Union (NYCLU) have expressed concerns over the policy's vagueness.[24] The NYCLU first expressed concern

[15] *See* Enrique Armijo, *Government-Provided Internet Access: Terms of Service as Speech Rules*, 41 FORDHAM URB. L.J. 1499, 1500–01 (2014).

[16] *See id.*; *see also* Lennard G. Kruger & Angele A. Gilroy, Cong. Research Serv., R44080, Municipal Broadband: Background and Policy Debate (2016).

[17] Sharon E. Gillett, *Municipal Wireless Broadband: Hype or Harbinger?*, 79 S. CAL. L. REV. 561, 571 (2006) ("[A] hotzone is a small geographic area, such as a public park, downtown shopping district, or city office building, in which wireless connectivity is made available.").

[18] *See* Armijo, *supra* note 11, at 1504.

[19] *See* Nicole A. Ozer, *Companies Positioned in the Middle: Municipal Wireless and Its Impact on Privacy and Free Speech*, 41 U. S.F. L. REV. 635, 639 (2007) (discussion of the Fourth Amendment was limited to the "Third Party Doctrine.").

[20] *See* Nicole A. Ozer, *No Such Thing As "Free" Internet: Safeguarding Privacy and Free Speech in Municipal Wireless Systems*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 519, 524 (2008); David Essex, *Cities make financial sense of WiFi projects*, GOV'T COMPUTER NEWS (Sept. 14, 2006)), https://gcn.com/Articles/2006/09/14/Cities-make-financial-sense-of-WiFi-projects.aspx. Both commentators argued that businesses, residents, and visitors increasingly expect high-speed Internet connections in public spaces, and city leaders seem to believe that if they don't build it, those businesses, residents, and visitors will not come.

[21] *See* Armijo, *supra* note 11, at 1504.

[22] *See* CITY OF N.Y. DEP'T OF INFO. TECH. & TELECOMM., EXHIBIT 2: CITYBRIDGE PRIVACY Policy (2017), http://www1.nyc.gov/assets/doitt/downloads/pdf/Proposed-PCS-Franchise-Exhibit-2-CityBridge-Privacy-Policy.pdf.

[23] *See* LinkNYC Launch, *supra* note 1.

[24] Letter from Mariko Hirose, Senior Staff Attorney, & Johanna New York Civil Liberties Union,

about the volume of private information CityBridge is retaining about its users, noting that "in order to register for the service LinkNYC users must submit their e-mail addresses and agree to allow CityBridge to collect information about what websites they visit on their devices, where and how long they linger on certain information on a webpage, and what links they click."[25] This is particularly worrisome given that a user's web history can reveal a wealth of information about his or her personal life.[26] The NYCLU next took exception with the lack of safeguards in place for government requests for information.[27] According to the NYCLU, LinkNYC's privacy policy should include a provision mandating that CityBridge inform users of any government requests for information using the email address that they provided during registration or through any other personally identifiable information in CityBridge's possession.[28] The NYCLU also took issue with CityBridge's data retention policy.[29] The privacy policy indicates that CityBridge will make "reasonable efforts to retain Personally Identifiable Information . . . provide[d] to us during registration no longer than 12 months after your last login."[30] However, this language could allow personal information to be retained indefinitely "so long as one uses the kiosks periodically," and that "12 months after your last login" is not the same as a twelve-month retention policy.[31]

The concerns expressed by the NYCLU raise many questions and may implicate both the First and Fourth Amendments. Existing scholarship has considered the constitutional concerns raised by municipal Wi-Fi programs in the context of the First Amendment[32] and, in only limited respects, the Fourth Amendment.[33] This Note will explore the obvious gap in scholarship examining the Fourth Amendment's application to municipal Wi-Fi programs. It explores Fourth Amendment jurisprudence regarding cases that specifically grapple with the public/private distinction in the Fourth Amendment's protections.

This Note begins by briefly surveying the Fourth Amendment's application in landmark modern-era Supreme Court cases and the accompanying issue of what constitutes a reasonable expectation of

to Maya Wiley, Counsel to the Mayor (March 15, 2016) (on file with New York Civil Liberties Union).

25 *Id.*

26 *See* Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014) (on file with author).

27 *See* Letter from Mariko Hirose & Johanna Miller, *supra* note 24, at 2.

28 *See id.* at 3.

29 *See id.* at 1.

30 *See id.* at 2.

31 *See id.*

32 *See* Armijo, *supra* note 15.

33 *See* Ozer, *supra* note 20, at 547.

privacy. Next, Section I.C. introduces the "third-party doctrine" which states, in brief, that there is no Fourth Amendment interest in information knowingly and voluntarily revealed to "third parties." Section I.D. will introduce the state-action doctrine. Section II examines whether the New York City government's actions in hiring CityBridge to administer the LinkNYC program were sufficient to implicate the state-action doctrine and trigger the Fourth Amendment's protections. Section III examines whether the LinkNYC Program implicates the third-party doctrine.

Though the LinkNYC program likely implicates the state-action doctrine, it is unlikely that a LinkNYC user would have any reasonable expectation of privacy due to the third-party doctrine. The state action doctrine and the third-party doctrine combine to create a scenario in which a municipality is able to escape Fourth Amendment scrutiny for information that it collects by operating through a nominal third party. The fact that the LinkNYC program provides an essential service for a segment of the population amplifies the perverse results of this situation, creating the potential for a two-tiered system of privacy rights in which rich New Yorkers are subject to different privacy policies than poor New Yorkers. Internet access is a necessity, and poor citizens cannot use it anywhere else. In this situation, poorer citizens who have no choice but to use the City-sponsored Wi-Fi will be subject to different standards than wealthier residents who contract with a private Internet Service Provider. Moreover, the existing privacy policy is insufficient to protect these interests, as it is merely a regulatory contract, and is thus insufficient to protect the weighty interests outlined above. Given these risks, this Note proposes that Congress amend the Electronic Communications Privacy Act (ECPA) or the courts read the ECPA to be applicable, without exception, to municipal Wi-Fi programs like LinkNYC. These changes would be sufficient to protect LinkNYC users' Fourth Amendment rights.

## I. THE FOURTH AMENDMENT TODAY

### A. *The "Property-Based Approach"*

The Fourth Amendment provides protection against government intrusion by barring "unreasonable searches and seizures."[34] However,

[34] U.S. Const. amend. IV. ("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."). For a detailed history of the origins of the Fourth Amendment, see Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 250–58 (2016).

the U.S. Supreme Court has often struggled to interpret the boundaries of these famous words. The Court's long-standing difficulties have led legal scholars to label the Court's Fourth Amendment jurisprudence as "'contentious' . . . [and] 'riddled with inconsistency and incoherence.'"[35] However, the concept that "a man [is able] to retreat into his own home and there be free from unreasonable governmental intrusion"[36] "is the oldest and most well-established strain of search and seizure law" and is "one of the rare well-defined rules of Fourth Amendment jurisprudence."[37] The Court used this "Property-Based Approach"[38] to apply the Fourth Amendment throughout the nineteenth century, but the advent of the telephone in the twentieth century eventually pushed the Court to rethink its analysis.[39] In *Olmstead v. United States*, the Court applied this antiquated framework to the arena of warrantless wiretapping.[40] The Court determined that the defendant was not entitled to Fourth Amendment protection from the wiretap, since "the intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[41] The Court subsequently applied the reasoning expounded in *Olmstead* to *Goldman v. United States*, holding that evidence of conversations obtained by use of technology-enabled eavesdropping did not violate the Fourth Amendment.[42] Justice Murphy's vigorous dissent in *Goldman* cast doubt on the Court's analysis, noting that the fact that modern surveillance methods did not require a physical intrusion into one's home was not decisive as "the privacy of the citizen is equally invaded by agents of the Government and intimate personal matters are laid bare to view"[43] by modern methods of surveillance.[44] In light of changing times, the Supreme Court had no choice but to reconsider its position in *Olmstead*.[45]

---

35 Colin Shaff, Is the Court Allergic to Katz? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test, 23 S. CAL. INTERDISC. L.J. 409, 410 (2014) (citing Daniel J. Solove, Fourth Amendment Pragmatism, 51 B.C. L. REV. 1511, 1511 (2010)).

36 Silverman v. United States, 365 U.S. 505, 511 (1961).

37 Price, *supra* note 34, at 258.

38 *Id.*

39 *Id.* at 258–59.

40 Olmstead v. United States, 277 U.S. 438, 465 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

41 *Id.*

42 Goldman v. United States, 316 U.S. 129, 135 (1942), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

43 *Id.* at 139 (Murphy, J., dissenting).

44 *See* Price, supra note 34, at 260–61.

45 *See id.*

### B. *The Reasonable Expectation of Privacy*

In order to determine that a search violated a citizen's reasonable right to privacy under the Fourth Amendment, the U.S. Supreme Court has embraced Justice Harlan's concurrence in *Katz v. United States*.[46] In *Katz,* the Court held that the government's use of an electronic device to listen to a conversation in a phone booth violated the privacy upon which the appellant justifiably relied while using the telephone booth.[47] Justice Harlan clarified the Court's methodology, and outlined a test containing a two-fold requirement: "first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[48] Notably, the Court announced that "the Fourth Amendment protects people, not places,"[49] thus making "a decisive shift away from the traditional concepts of property and trespass that had long dominated its jurisprudence."[50]

### C. *The Third-Party Doctrine*

"The third-party doctrine is a product of pre-digital era case law."[51] In *United States v. Miller*, federal authorities served subpoenas on two banks where the defendant Miller maintained accounts, requesting "all records of accounts, i.e., savings, checking, loan or otherwise."[52] The Court held that citizens have no expectation of privacy in financial information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[53] The Court reasoned that individuals must assume the risk that information voluntarily provided to third parties will be disclosed to others.[54]

The Court expanded on the third-party doctrine in *Smith v. Maryland*.[55] In that case, the Court upheld law enforcement's use of a pen register to monitor outgoing calls from a suspect's residence, given that he had no reasonable expectation of privacy in the numbers he

46 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring in judgment).
47 *Id.* at 353.
48 *Id.* at 361 (Harlan, J., concurring in judgment).
49 *Id.* at 351.
50 Price, *supra* note 34, at 261.
51 *See* Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 CARDOZO L. REV. DE NOVO 119, 121 (2015).
52 United States v. Miller, 425 U.S. 435, 437 (1976).
53 *Id.* at 442.
54 *Id.*
55 Smith v. Maryland, 442 U.S. 735 (1979).

dialed.[56] The Court reasoned that the defendant was aware that his phone records would be conveyed to the telephone company to connect his call, and that even if he did possess a subjective expectation of privacy, it was not one which society would be prepared to recognize as reasonable.[57] Together, *United States v. Miller* and *Smith v. Maryland* "are known for the rule that there is no Fourth Amendment interest in information knowingly and voluntarily revealed to 'third parties.'"[58] Scholars have (often pejoratively) called this approach the "binary conceptualization of privacy."[59]

Courts have extended the principle expounded in *Miller* to cases involving business records, public utility records in telephone tolling records,[60] and records indicating home electricity usage.[61] Recently, the Court has struggled to apply the existing third-party doctrine framework in a modern context.[62] In *United States v. Jones*, the Court held that the government's use of a GPS tracking device to monitor a suspect's location on public roads for twenty-eight days constituted a search under the Fourth Amendment.[63] Five Justices suggested that the length of the surveillance violated a societal expectation of privacy, notwithstanding the fact that the suspect's vehicle was traveling on public roads and readily observable.[64] Justice Sotomayor directly questioned the validity of the third-party doctrine as it stands today, writing:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a

[56] *Id.*
[57] *Id.*
[58] Price, *supra* note 34, at 265.
[59] *See* Natasha H. Duarte, *The Home Out of Context: The Post-Riley Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1143, 1146 (2015); *see also* Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 377 (2013); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1151 (2002).
[60] United States v. Covello, 410 F.2d 536, 542 (2d Cir. 1969) (holding that telephone subscribers are "fully aware that . . . records will be made" of their toll calls and have no reasonable expectation to privacy.").
[61] *See* Duarte, *supra* note 59, at 1141, 1157 (collecting cases).
[62] *See* U.S. v. Jones, 565 U.S. 400, 404 (2012).
[63] *Id.* at 404.
[64] *Id.*

> limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[65]

Justice Sotomayor's concurrence in *Jones* echoes Justice Harlan's dissent in *United States v. Whit*e.[66] In *White*, the Supreme Court held that government recording of conversations using concealed radio transmitters worn by informants does not violate the Fourth Amendment and, thus, does not require a warrant.[67] In his famous dissent, Justice Harlan argued that one's expectation of privacy should be balanced against the utility as a technique of law enforcement "[t]o the likely extent of its likely impact on individual's sense of security."[68] Alluding to "the Orwellian Big Brother," he wrote that warrantless "electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society," and dissented on the grounds that the risks of the electronic listener or observer should not be imposed on citizens "without at least the protection of a warrant requirement."[69]

### D. *The State Action Doctrine*

"Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government."[70] Since its inception in the Court's Civil Rights Cases in 1883,[71] the state-action doctrine has launched a "judicial search for governmental responsibility in all cases in which the controlling issue becomes whether government is in some way responsible for the particular harm" that a private party inflicted on another.[72] To establish state action, a plaintiff's grievance must have been "caused by the exercise of some right or privilege created by the State or by a rule of conduct imposed by the State or by a person for whom the State is responsible."[73] In addition, "the party

---

65 *Id.* at 417–18 (Sotomayor, J., concurring).
66 United States. v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).
67 *Id.* at 749.
68 *Id.* at 787 (Harlan, J., dissenting).
69 *Id.*
70 *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 614 (1989).
71 Civil Rights Cases, 109 U.S. 3, 11 (1883) (holding that Fourteenth Amendment guarantees civil rights against state aggression, not wrongful acts of individuals).
72 G. Sidney Buchanan, *A Conceptual History of the State Action Doctrine: The Search for Governmental Responsibility*, 34 HOUS. L. REV. 333, 344 (1997). "While every state function or service—housing, education, health care, policing, welfare, transportation, postal service, and dispute resolution—has a private counterpart, the law subjects only state actors to constitutional limits. The traditional justification for this differential treatment is that government power is uniquely coercive." Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 576 n.114 (2000) (citation omitted).
73 Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982).

charged with the deprivation must be a person who may fairly be said to be a state actor."[74] A state actor is not necessarily a public official, but someone who has "acted together with or has obtained significant aid from state officials, or . . . [someone whose] conduct is otherwise chargeable to the State."[75] State action "implies governmental action at any level - federal, state, or municipal."[76]

The Supreme Court has historically used three tests in evaluating state action: (i) the public function test; (ii) the state compulsion test;[77] and (iii) the nexus/joint action test.[78] The public function test for state action has been limited strictly and covers only private actors performing functions that are "traditionally the exclusive prerogative of the State."[79] The state compulsion test limits state action to instances in which the government has coerced or at least significantly encouraged the action alleged to violate the Constitution.[80] Under the nexus/joint action test, a plaintiff must demonstrate that "the State had so far insinuated itself into a position of interdependence with the [private party] that it was a joint participant in the enterprise."[81] These tests are alternatives—satisfaction of any of which independently establishes state action.[82] Moreover, the test is binary in its application, "what falls on the public side suffers every constitutional constraint, while what falls on the private side operates unfettered."[83] The State Action Doctrine has caused significant confusion among commentators[84] and the Court itself, leading the Court to question "[w]hether these different tests are actually different in operation or simply different ways of characterizing the necessarily fact-bound inquiry that confronts the

[74] *Id.*

[75] *Id.*

[76] Julie K. Brown, *Less Is More: Decluttering the State Action Doctrine*, 73 MO. L. REV. 561, 561 n.2 (2008).

[77] *See id.* at 565 (citing Blum v. Yaretsky, 457 U.S. 991, 1004 (1982)) (Under the state compulsion test, more than "mere approval or acquiescence in the initiatives of the private party is necessary to hold the state responsible for those initiatives under the terms of the Fourteenth Amendment.")). When applying the state compulsion test, the court considers, "[t]he state's influence over the private actor and, therefore, its potential application is much broader than the public function test." *Id.* at 566. Under this test, courts are primarily concerned with "whether or not the private entity had a choice to act or refrain from acting."). *Id.*

[78] *See Nat'l Broad. Co.*, 860 F.2d at 1026.

[79] *Id.*

[80] *See id.* Given the state compulsion test's inapplicability to this issue, this Note will limit its discussion of state action to the public function and joint nexus tests.

[81] *Nat'l Broad. Co.*, 860 F.2d at 1026–27.

[82] *See* Freeman, *supra* note 72 at 578 (2000); Lugar v. Edmondson Oil Co., 457 U.S. 922, 939 (1982) (As the Supreme Court stated, "[w]hether these different tests are actually different in operation or simply different ways of characterizing the necessarily fact-bound inquiry that confronts the Court in such a situation need not be resolved here.")

[83] Freeman, *supra* note 72, at 581.

[84] *See e.g.*, John Dorsett Niles et. al., *Making Sense of State Action*, 51 SANTA CLARA L. REV. 885, 886 (2011); Christopher W. Schmidt, *On Doctrinal Confusion: The Case of the State Action Doctrine*, 2016 B.Y.U. L. REV. 575, 584 (2016); Buchanan, *supra* note 72, at 352.

Court in such a situation."[85]

## II. THE LINKNYC PROGRAM UNDER THE STATE ACTION DOCTRINE

The following section considers the LinkNYC program as it exists now under the historical tests to determine state action: the public function test, the state compulsion test, and the nexus/joint action test.[86]

### A. *The Public Function Test*

The public function test for state action has historically been strictly limited, covering only private actors performing functions "traditionally the exclusive prerogative of the State."[87] Providing high-speed Internet is likely not an exclusive "traditional state function[,]"[88] and the LinkNYC program may not fall within the public function test on that basis alone. The fact that providing Internet is not an "exclusive traditional state function" should not be dispositive as the Supreme Court assumes a "duty to see that [the Fourth Amendment] . . . receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation."[89]

Moreover, even if furnishing a public Wi-Fi service is clearly not an "exclusive" traditional government function,[90] we are living "in a time where the daily necessities of life and work demand . . . internet access."[91] Commentators have come to view "[b]roadband connectivity [as] . . . the new critical infrastructure of the 21st century"[92] arguing that "[h]igh-speed [Internet] access should no longer be considered a commodity, *but rather a critical utility on par with water and electricity*."[93]

---

85 *Lugar*, 457 U.S. at 939.

86 *See* Buchanan, *supra* note 72, at 388.

87 Jackson v. Metro. Edison Co., 419 U.S. 345, 353 (1974); *see also* Rendell-Baker v. Kohn, 457 U.S. 830, 842 (1982).

88 *See* Armijo, *supra* note 11, at 433.

89 *See* Price, *supra* note 34, at 271–72 (arguing that Fourth Amendment "papers" should expand to include data held by a third party). "[C]onsider the evolution of the Supreme Court's jurisprudence on 'houses.' A literal reading of the term could limit the scope of the Fourth Amendment quite significantly. *Id.* at 271. Price continued: "Yet the Court has consistently extended constitutional protection far beyond the four walls of a private residence. . . . Instead, the Court assumes a 'duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation.' *Id.* at 271–72 (citations omitted).

90 *See* Armijo, *supra* note 11 at 433.

91 United States v. Albertson, 645 F.3d 191, 200 (3d Cir. 2011).

92 Sascha D. Meinrath, et al., *Digital Feudalism: Enclosures and Erasures From Digital Rights Management To The Digital Divide*, 19 COMMLAW CONSPECTUS 423, 478 (2011).

93 *Id.* at 477 (emphasis added).

The Federal Communications Commission (FCC) under the Obama Administration accepted this argument and declared that ISPs are common carriers, lending further support to the proposition that Wi-Fi is a public utility.[94] In an effort to compel "net neutrality,"[95] the FCC promulgated an order in which it reclassified broadband service as a telecommunications service, which are subject to common carrier regulation under Title II of the Communications Act of 1934.[96] Broadband ISPs and industry associations petitioned the Court of Appeals for the District of Columbia Circuit for review of the FCC order.[97] The Circuit Court upheld the regulation, noting that the FCC had properly defined broadband service as a "telecommunications services," and therefore, the regulation was within its purview.[98]

However, the FCC reversed its stance on net neutrality soon after President Trump took office, and sought to repeal the Obama era net neutrality regulations by reclassifying broadband Internet as an "information service," thus removing broadband internet from common carrier regulation under Title II of the Communications Act of 1934.[99] The FCC's proposed re-classification of broadband internet was met with intense public outrage.[100] Despite the widespread public disapproval and allegations that the FCC public comment process was tainted by fake comments,[101] the FCC, under Chairman Ajit Pai, voted to reclassify broadband Internet as an "information service," thereby

[94] *See* In the Matter of Protecting & Promoting the Open Internet, 30 F.C.C. Rcd. 5601 (2015) (citing The Communications Act of 1934, 47 U.S.C. §151 (2012)).

[95] "Net neutrality" is the common name of an effort to compel broadband providers to treat all Internet traffic the same regardless of source. *See* Verizon v. F.C.C., 740 F.3d 623, 628 (D.C. Cir. 2014).

[96] *See* In the Matter of Protecting & Promoting the Open Internet, 30 F.C.C. Rcd. 5601 (2015) (citing The Communications Act of 1934, 47 U.S.C. §151 (2012)).

[97] *See* United States Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016).

[98] *See id.* This case marked the FCC's third attempt in seven years at achieving net neutrality. The D.C. Circuit Court of Appeals struck down the FCC's first attempt in Comcast Corp. v. FCC, 600 F.3d 642, 661 (D.C. Cir. 2010), because the "Commission had failed to cite any statutory authority that would justify its order compelling a broadband provider to adhere to certain open internet practices." In Verizon v. FCC, 740 F.3d 623, 650 (D.C. Cir. 2014), the Court of Appeals for the D.C. Circuit acknowledged the FCC's right to enact net neutrality rules yet denied the FCC's second attempt to do so since the rules classified broadband service as an "information service" which was outside the scope of protection under The Communications Act of 1934 which only extended to "telecommunications" services.

[99] *See* In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, Notice of Proposed Rulemaking, 32 FCC Rcd. 4434 at *7 (2017).

[100] *See* Cecilia Kang, *Net Neutrality Hits a Nerve, Eliciting Intense Reactions*, N.Y. TIMES (Nov. 28, 2017), https://www.nytimes.com/2017/11/28/technology/net-neutrality-reaction.html; Cecilia Kang, *F.C.C. Plans Net Neutrality Repeal in a Victory for Telecoms*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/fcc-net-neutrality.html.

[101] *See* Press Release, Office of the New York State Attorney General, A.G. Schneiderman Releases New Details On Investigation Into Fake Net Neutrality Comment (Dec. 13, 2017), https://ag.ny.gov/press-release/ag-schneiderman-releases-new-details-investigation-fake-net-neutrality-comments.

eviscerating net neutrality regulations.[102] The ruling is currently being challenged by twenty-two state attorneys general, who have attacked the FCC's action as "arbitrary, capricious, and an abuse of discretion."[103]

In light of the Supreme Court's latest jurisprudence, the issue of whether broadband Internet enjoys protection as a common carrier could be crucial for future application of the public function test. By the 1980s, the public function test had found state action so infrequently that it had become "[an] impotent formality in which the Court inevitably finds that the private action in question lacks 'the feature of exclusivity.'"[104] In *Edmonson v. Leesville Concrete Co.*, the Court considered the question of "whether a private litigant in a civil case may use peremptory challenges to exclude jurors on account of their race."[105] The Court framed the public function issue in terms of "whether the actor is performing a traditional governmental function."[106] Notably, the Court left out the word "exclusive," which can be interpreted as a departure from the exclusivity requirement of previous public function cases:[107]

> In the wake of this ruling, "[m]ore recent decisions have turned away from an "all or nothing question of governmental exclusivity" to a more nuanced public function analysis, as well as a willingness to consider the combined weight of public function along with other state action factors like entwinement."[108]

As discussed above, the Internet is becoming an essential part of modern life. A chorus of New York City elected officials echoed this sentiment at the LinkNYC press conference.[109] At its core, the

[102] *See* In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, WC Docket No. 17-108, FCC 17-166 (released on Jan 4, 2018).

[103] State of New York, et al. v. Federal Communications Commission, et al., No. 18-1013, at *2 (D.C. Cir. filed Jan. 16, 2018); *see also* Press Release, Office of the New York State Attorney General, A.G. Schneiderman Files Suit To Stop Illegal Rollback Of Net Neutrality (Jan. 16, 2018), https://ag.ny.gov/press-release/ag-schneiderman-files-suit-stop-illegal-rollback-net-neutrality; Cecilia Kang, *States Push Back After Net Neutrality Repeal*, N.Y. TIMES (Jan. 11, 2018), https://www.nytimes.com/2018/01/11/technology/net-neutrality-states.html.

[104] *See* Buchanan, *supra* note 72, at 388–89.

[105] Edmonson v. Leesville Concrete Co., 500 U.S. 614 (1991).

[106] *Id.*

[107] *See* Buchanan, *supra* note 72, at 388.

[108] *See* Armijo, *supra* note 15, at 1520 ("Entwinement" is another term of art to reference the Joint Nexus Test.).

[109] *See* LinkNYC Launch, *supra* note 1. Manhattan Borough President Gale A. Brewer: "Wireless internet is the key public utility for the digital age. It's hard to overstate how revolutionary delivering free, accessible Wi-Fi to New York City's neighborhoods will be." Brooklyn Borough President Eric L. Adams: "Reliable, high-speed wireless connections are now fundamental to our economy and our entire civil society. Bronx Borough President Ruben Diaz Jr: "Our mobile devices, tablets, and computers have become an integral part of our lives… [w]e fought hard to make sure a digital divide was not created in this city, making sure all five boroughs would benefit from being able to access high-speed Internet through the LinkNYC program." Queens Borough President Melinda Katz: "Free public internet access is more than just

LinkNYC program is an attempt to advance societal welfare by "leveling the playing field and providing every New Yorker with access to the most important tool of the 21st century."[110] These goals are "bedrock public purposes"[111] and should be considered government functions sufficient to active the state-action doctrine. Moreover, courts are to consider the public function test in conjunction with "other state action factors like entwinement."[112] It is through this examination that the scale is tipped even further in favor of state action sufficient to implicate Fourth Amendment protections for LinkNYC users.

### B. *The Joint Nexus Test*

Under the joint nexus test, a plaintiff must demonstrate that "the State had so far insinuated itself into a position of interdependence with the [private party] that it was a joint participant in the enterprise."[113] In *Burton v. Wilmington Parking Authority*, a private lessee—who practiced racial discrimination—leased space for a restaurant from a state parking authority in a publicly-owned building.[114] The Court held that the State had so far insinuated itself into a position of interdependence with the restaurant that it was a joint participant in the enterprise.[115] The Court explicitly limited its holding to "lessees of public property."[116]

Pursuant to the franchise agreement governing LinkNYC's expansion around the city, CityBridge must pay the City of New York a "franchise fee."[117] The franchise fee is "an amount equal to the greater of . . . fifty percent (50%) of Gross Revenues for that Contract Year or the Minimum Annual Guarantee payment," which ranges from $20,000,000 in contract year one to $70,932,000 in contract year fifteen.[118] Though public-private contracts for service delivery are not sufficient on their own to make a private party a state actor,[119] CityBridge's franchise agreement may make it a "lessee" under *Burton*.[120] The counter-argument that CityBridge does not own or pay

a leisurely perk. It's an indicator of economic growth, recognized potential and a way to help bridge the Digital Divide already predisposed to income inequalities." *Id*.

110 *Id.*

111 *See* Armijo, *supra* note 15, at 1520.

112 *Id.*

113 *See* Nat'l Broad. Co. v. Commc'ns Workers of Am., AFL-CIO, 860 F.2d 1022, 1026 (11th Cir. 1988).

114 Burton v. Wilmington Parking Authority, 365 U.S. 715, 719 (1961).

115 *Id.* at 725.

116 *Id.* at 726.

117 *See* CityBridge Franchise Agreement, *supra* note 5.

118 *Id.*

119 *See* Armijo, *supra* note 15, at 1520 (citing Dickerson v. Cal. Waste Solutions, 2009 WL 2913452 (N.D. Cal. Sept. 8, 2009)).

120 *See Burton*, 365 U.S. 715; CityBridge Franchise Agreement, *supra* note 5.

any rent under the agreement is not inconsistent with this conclusion. The franchise agreement is a contract requiring a predetermined percentage of total revenue in consideration for using city-owned land that was formerly the site of public telephones, which may place the situation in the purview of *Burton.*[121] However, the Supreme Court has stated that private use of public property, without more, is insufficient to find a close nexus.[122]

Notably, recent Supreme Court jurisprudence has evidenced a "returning willingness by the Court to consider the combined weight of all state contact factors under [the] state nexus analysis."[123] This test was articulated in *Lugar v. Edmondson Oil Co.*:

> In order to find a deprivation fairly attributable to the State, "First, the deprivation must be caused by the exercise of some right or privilege created by the State or by a rule of conduct imposed by the state or by a person for whom the State is responsible. . . Second, the party charged with the deprivation must be a person who may fairly be said to be a state actor."[124]

In *Edmonson v. Leesville Concrete Co., Inc*, the Court applied the two prong *Lugar* test for determining the existence of state action through a joint nexus.[125] On the first prong, the Court held that the use of peremptory challenges clearly constituted "the exercise of a right or privilege having its source in state authority" since the litigants used the court system to enforce this right.[126]

The Court then moved to the second prong of the *Lugar* test, stating additional relevant criteria to consider in conducting the joint nexus test.[127] The Court added that "it is relevant to examine the following: the extent to which the [private] actor relies on governmental assistance and benefits; . . . whether the actor is performing a traditional governmental function; . . . and whether the injury caused is aggravated in a unique way by the incidents of governmental authority."[128] Applying these new criteria, the Court determined that "a private party could not exercise its peremptory challenges absent the overt, significant assistance of the court."[129] The Court repeated this analysis in an almost identical form in a later case.[130]

As discussed above, the goals of the LinkNYC constitute "bedrock

---

121 *See Burton*, 365 U.S. at 715.
122 *See* Brown, *supra* note 76, at 566 (citing Blum v. Yaretsky, 457 U.S. 991 (1982)).
123 *See* Buchannan, *supra* note 72, at 422–23.
124 Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982).
125 Edmonson v. Leesville Concrete Co., 500 U.S. 614, 620 (citing *Lugar*, 457 U.S. at 937).
126 *Id.*
127 *Id.*
128 Buchannan, *supra* note 72, at 421 (citing *Leesville Concrete Co.*, 500 U.S. at 621–22).
129 *Leesville Concrete Co.*, 500 U.S. at 624.
130 *See* Buchannan, *supra* note 72, at 389 (citing Georgia v. McCollum, 505 U.S. 42, 51 (1992)).

public purposes," and should considered government functions sufficient to satisfy the first prong of *Lugar* test. Similarly to the litigants in *Edmonson*, CityBridge could not operate its business without the de facto monopoly granted to it by the City of New York. This fact has led several scholars to determine that municipal Wi-Fi systems may implicate state action in and of itself.[131] The second prong of the *Lugar* test is easily satisfied by considering the additional *Leesville* factors.[132]

## III. THE LINKNYC PROGRAM UNDER THE THIRD-PARTY DOCTRINE

A federal court analyzing the LinkNYC program under the third-party doctrine is likely to apply the public utility framework, as recent case law has deemed broadband service a "telecommunications service."[133] Yet, the quantity and quality of private information that can be collected from a LinkNYC user is sufficient grounds for distinguishing it from the traditional public utility analysis. The franchise agreement governing LinkNYC's proliferation requires that CityBridge "not collect any such Personally Identifiable Information concerning any User except to the extent necessary for technical management of the Wi-Fi service."[134] Yet, this vague language begs the question of what is personally identifiable information.

Courts have attempted to draw a distinction between the metadata, otherwise known as information other than the actual substance of the communication,[135] and the content of electronic activity. In *United States v. Warshack*, the United States Court of Appeals for the Sixth Circuit considered whether a user has a reasonable expectation of privacy in the content of his or her e-mails stored on third party servers.[136] The *Warshack* court held that a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP."[137] Notably, the court distinguished *Miller* on two grounds.[138] First, *Miller* involved

131 "When there is state action through municipally owned or supported systems, constitutional rights must be safeguarded." Ozer, *supra* note 24 at 551. "[I]f a municipality claims to provide high-speed Internet service to members of the public in its own name, and the municipality has pointed to important public purposes in delegating authority to the service-provider-in-fact, then the Constitution's demands should apply to that service." Armijo, *supra* note 15, at 1520. These arguments apply in the context of the LinkNYC Program as well.

132 *See* Leesville Concrete Co., 500 U.S. at 620–21.

133 *See* discussion *supra* Section I.C.

134 CityBridge Franchise Agreement, *supra* note 5, at § 4.4.4(iii).

135 *See* Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data about "the People,"* 2009 COLUM. BUS. L. REV. 950, 977 n.105 (2009).

136 United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010).

137 *Id.* at 288.

138 *Id.* at 287–88.

business records "as opposed to the potentially unlimited variety of 'confidential communications' at issue here."[139] Second, unlike the "bank depositor in *Miller* [who] conveyed information to the bank so that the bank could put the information to use 'in the ordinary course of business'", the defendant received his emails through an ISP who was not the intended recipient of the emails.[140]

In *United States v. Forrester*, the United States Court of Appeals for the Sixth Circuit considered whether the use of computer surveillance techniques that revealed data including the addresses of the sender and recipient of emails, the "IP addresses of websites [that defendant had] visited, and the total amount of data transmitted to or from defendant's Internet account" violated the Fourth Amendment.[141] The court analogized the email surveillance to surveillance of traditional mail, noting that "[t]he privacy interests in . . . [mail and email] . . . are identical."[142] The court embraced the traditional rule that the government "can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties."[143] The court reasoned that "[e]-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location," which is not entitled to have Fourth Amendment protection.[144] Notably, the court reserved the question of whether surveillance techniques that enable the government to determine the Uniform Resource Locator ("URL")[145] of the pages visited violate the Fourth Amendment.[146] The court reasoned that a "URL, unlike an IP address,[147] identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity."[148]

In contrast, courts have determined that metadata is not entitled to Fourth Amendment protection.[149] Yet, numerous scholars have noted

139 *Id.* at 288.
140 *Id.*
141 *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).
142 *Id.* at 511.
143 *Id.*
144 *Id.*
145 OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/url (A URL is the address of a World Wide Web page).
146 *Forrester*, 512 F.3d. at 510 n.6.
147 An "IP address" is a "unique numerical address identifying each computer on the [I]nternet." "A website typically has only one IP address even though it may contain hundreds or thousands of pages. For example, Google's IP address is 209.85.129.104 and the New York Times' website's IP address is 199.239.137.200." *See id.* at 510 n.5.
148 *Id.* at 504; "[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. This would reveal content . . . . " *Id.* at 504 (citing *Pen Registers Application*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)).
149 *See* United States v. DiTomasso, 56 F. Supp. 3d 584, 596 n.84 (S.D.N.Y. 2014) ("Unlike the content of chats, IP addresses are metadata, in which . . . [a user] would have a far more limited expectation of privacy, if any."). *See also* Freedman v. America Online, Inc., 412 F. Supp. 2d

that metadata is able to reveal a wealth of information about a user. For that reason, it should be considered as user content and subject to Fourth Amendment protections.[150] Moreover, as Justice Sotomayor notes in her concurrence in *Jones*,[151] metadata can be used to discern "political and religious beliefs, sexual habits, and so on."[152] The information collected by CityBridge implicates the same concerns as expressed by Justice Sotomayor in *Jones*:

> The [CityBridge] privacy policy provides that in order to register for the service LinkNYC users must submit their e-mail addresses and agree to allow CityBridge to collect information about what websites they visit on their devices, where and how long they linger on certain information on a webpage, and what links they click.[153]

The data collected by CityBridge can reveal precisely the same type of information that concerned Justice Sotomayor in *Jones*.[154] Information indicative of the length of time that a user hovers over a certain portion of an article can give authorities a wealth of information about the user such that it should be considered content and thus be protected by the Fourth Amendment.[155] However, in spite of these legitimate concerns, the vast majority of case law concerning the third party doctrine in the digital age would not entitle a LinkNYC user to a reasonable expectation of privacy for his or her metadata.[156]

The controversy surrounding smart meters[157] is instructive on this issue. Smart meters "collect fine-grained, minute-by-minute data about electricity use and transmit it back to the utility at regular intervals."[158] In *Naperville Smart Meter Awareness v. City of Naperville*, a non-profit corporation that opposed the city's replacement of analog electricity meters with smart meters brought suit, alleging, *inter alia*, violations of its members' right to freedom from unreasonable search or invasion of

174, 181 (D. Conn. 2005).

150 *See e.g.*, Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391 (2014); Price, *supra* note 34, at 284; Duarte, *supra* note 59, at 1143.

151 *See* discussion *supra* Section I.C.

152 U.S. v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

153 Hirose, *supra* note 24, at 1.

154 *See* CityBridge Franchise Agreement, *supra* note 5.

155 *See* Tene, *supra* note 150, at 424.

156 *See* United States v. Stanley, 753 F.3d 114 (3d Cir. 2014) (holding that an Internet user has no reasonable expectation to privacy in his internet history); United States v. Rigmaiden, 2013 WL 1932800, at *1 (D. Ariz. 2013) (holding that an Internet user had no reasonable expectation of privacy to information collected through his use of a wireless aircard, historical cell-site information and destination IP addresses).

157 Smart meters are "electronic utility meters that enable two-way communication between utilities and consumers." Duarte, *supra* note 59, at 1140 n.1 (citing *Advanced Metering Infrastructure and Customer Systems*, SMARTGRID.GOV (Sept. 2016), https://energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf (last visited Nov. 19, 2016)).

158 Duarte, *supra* note 59, at 1140.

their privacy under the Fourth Amendment.[159] The United States District Court for the Northern District of Illinois rejected this argument, holding that "the purported ability of smart meters to provide a 'constant conversation' . . . between the City and its customers does not establish beyond mere 'speculation' that the City has or will 'plausibly' use such information in an unconstitutional manner."[160] Any prospective litigant bringing suit against CityBridge or the City of New York may face the same problem as the plaintiff in *Naperville*: the fact that the technology exists does not automatically mean that it was used in an unconstitutional manner.[161]

The evolution of common-law treatment of cellphone surveillance is further evidence of the third-party doctrine's inapplicability to the modern world. Since the advent of cell phones, law enforcement has sought to surveil them.[162] Cell phones were traditionally monitored through a process which some have labeled as "carrier-assisted surveillance[,]"[163] which "can reveal a phone's historical,[164] current, or prospective location . . . as well as other types of data, such as numbers called and the addresses of web pages viewed from a mobile device."[165] The government may obtain historical or future CSLI with the aid of a cell phone carrier through either "a conventional warrant, or through a court order as outlined in § 2703(d)" of the SCA, which only requires the agents to "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of . . . [the] information sought, [is] relevant and material to an ongoing criminal investigation."[166]

---

159 *See* Naperville Smart Meter Awareness v. City of Naperville, 114 F. Supp. 3d 606, 613 (N.D. Ill. 2015).

160 *See id.* at 612 (internal citations omitted).

161 *See id.*

162 *See* Kristin Finklea, Encryption and Evolving Technology: Implications For U.S. Law Enforcement Investigations, CONG. RESEARCH SERV. (Feb. 18, 2016), https://fas.org/sgp/crs/misc/R44187.pdf.

163 *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 145 (2013–2014) (internal citations omitted). Carrier assisted surveillance is also known as "Cell Site Location Information" (CSLI). United States v. Lambis, 197 F. Supp. 3d 606, 608 (S.D.N.Y. 2016) ("CSLI is a record of non-content-based location information from the service provider derived from 'pings' sent to cell sites by a target cell phone.").

164 Government access to historical CSLI is regulated by a subsection of the Electronic Communications Privacy Act (ECPA) (discussed in detail below) called The Stored Communications Act (SCA) 18 U.S.C. §§ 2701–2711 (2012) and by the Fourth Amendment. *See* Zachary Ross, *Bridging the Cellular Divide: A Search for Consensus Regarding Law Enforcement Access to Historical Cell Data*, 35 CARDOZO L. REV. 1185, 1197–98 (2014). Under the SCA, through either a conventional warrant, or through a court order which only requires them to "offer specific and articulable facts" demonstrating that the information sought is "relevant and material to an ongoing criminal investigation." *Id.* at 1198–99.

165 *See* Pell, *supra* note 163, at 145.

166 *See* Ross, *supra* note 164 at 1198–99 (quoting 18 U.S.C. §2703(c)(1)–(d)).

The newest surveillance device to utilize cell phone networks are cell-site simulators, which are sometimes referred to as "StingRay," "Hailstorm," or "TriggerFish" and differ from traditional cell phone surveillance in many respects.[167] A StingRay is a device that locates cell phones by mimicking the service provider's cell tower (or "cell site") and forcing cell phones to transmit "pings"[168] to the simulator.[169] The device then calculates the strength of the "pings" until the target phone is pinpointed.[170] To use a StingRay, the federal government typically bases its application on the Pen Register Statute[171] and must only confirm "that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[172] However, StingRays are often used without any court approval.[173]

StingRay devices are so intrusive that the United States Department of Justice (DOJ) changed its internal policies and now requires government agents to obtain a warrant before utilizing a cell-site simulator.[174] While it is certainly a step in the right direction, this policy only applies to Federal Law Enforcement Officers.[175] Additionally, the DOJ policy notes exceptions "for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable."[176]

Similarly to the DOJ, courts have begun to reign in StingRay programs as well, with important ramifications for the third-party Doctrine.[177] In *State v. Andrews*, the Court of Special Appeals of Maryland considered whether evidence obtained pursuant to warrantless use of a StingRay device violated the Fourth Amendment and should be

167 *Lambis*, 197 F. Supp. 3d at 609. Though cell site simulators go by many names, this Note will refer to them by their most popular name, StingRay.

168 A ping "is a signal sent to a cellphone to locate it by its global positioning system." Devega v. State, 689 S.E.2d 293, 299 (Ga. 2010).

169 *See Lambis*, 197 F. Supp. 3d at 609.

170 *See id.* For a detailed discussion of how StingRays function, see Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75, 76–77 (2015).

171 18 U.S.C. § 3121 (2012).

172 *See* Owsley, *supra* note 170, at 81.

173 *See e.g.*, Thomas v. State, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013). The Supreme Court will soon determine the issue of whether the warrantless search and seizure of cell phone records violates the Fourth Amendment. *See* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16-402).

174 *See* Press Release, DOJ, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015).

175 *See* Tal Kopan & Josh Gaynor, *DOJ Cracks Down on Use of Cell-Duping Stingrays*, CNN, Sept. 3, 2015, *available at* http://edition.cnn.com/2015/09/03/politics/stingrays-cell-site-simulator-justice-department-rules.

176 *Id.*

177 *See* Cindy D. Ham, *How Lambis and Csli Litigation Mandate Warrants for Cell-Site Simulator Usage in New York*, 95 WASH. U.L. REV. 509, 528 (2017); State v. Andrews, 227 Md. App. 350 (Md. Ct. Spec. App. 2016); United States v. Lambis, 197 F. Supp. 3d 606, 606.

suppressed.[178] The court held that people have "a reasonable expectation that their cell phones will not be used as real-time tracking devices" by law enforcement and an objectively "reasonable expectation of privacy in real-time cell phone location information."[179] The court next responded to the state's argument that the third-party Doctrine obviated the need for a warrant.[180] The court noted that, through its use of the StingRay, the defendant did not voluntarily share his cell site location information with his cell phone provider, and thus, under third-party doctrine, defendant did not forfeit his reasonable expectation of privacy in such information.[181] The court concluded by writing that "it cannot be said that Andrews "assumed the risk" that the information obtained through the use of the Hailstorm device would be shared by the service provider as in Smith."[182]

In *United States v. Lambis*, the United States District Court for the Southern District of New York considered whether evidence obtained pursuant to warrantless use of a StingRay violated the Fourth Amendment.[183] Judge Pauley held that the search violated the Fourth Amendment, writing that, "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device" and suppressed all evidence obtained through the StingRay.[184] Judge Pauley drew the same distinction that the Maryland Court of Special Appeals drew in *Andrews*: writing that, unlike "pen register information or CSLI, *a cell-site simulator does not involve a third party*."[185]

The distinctions drawn by the *Andrews* and *Lambis* courts regarding who is collecting the information could prove to be crucial in the context of the LinkNYC case. As discussed in Section I.C, the LinkNYC program implicates state action and CityBridge is, at best, a nominal third party.[186] Considering this fact, LinkNYC is similar to the StingRay at issue in *Lambis* and *Andrews* as *none of these collection methods involves a third party*. Additionally, the planned ubiquity of Links around New York City worsens the fears outlined by the *Lambis* and *Andrews* courts. The City has authorized at least 7,500 Links – and as many as 10,000 across the five boroughs.[187] To accomplish its goal of 7,500 Links across the City, CityBridge likely will place individual

178 *See Andrews*, 227 Md. App. at 354.
179 *Id.* at 393, 394–95.
180 *Id.*
181 *Id.* at 398–99.
182 *Id.* at 401.
183 *See* Lambis, 197 F. Supp. 3d at 606. In *Lambis*, The Drug Enforcement Agency, (DEA) a Federal Agency, used the StingRay before the DOJ changed its policy.
184 *Id.* at 611.
185 *Id.* at 616 (emphasis added).
186 *See* discussion *supra* Section I.C.
187 *See* CityBridge Franchise Agreement, *supra* note 5.

Links within close proximity to each other.[188] Given this and the fact that devices automatically connect to LinkNYC once registered,[189] it is possible that a user may always be connected to the LinkNYC network. The LinkNYC program has the potential to track its users and retain its findings for at least twelve months[190] and will implicate the same concerns expressed in *Lambis* and *Andrews*.

While the courts have only recently joined the debate, an unlikely group has long since banded together to protect rights to privacy: corporate America. When Edward Snowden exposed the National Security Agency's (NSA) mass surveillance programs which entailed "dragnet data collection of American citizens,"[191] he spawned a "significant public reassessment of surveillance practices by the American security establishment."[192] While this debate raged, smartphones[193] became ubiquitous in the United States.[194] Smartphones contain detailed records about their users:

> . . . including cell phone records that indicate which cell tower was used in making or receiving a call; Global Positioning System (GPS) location points, stored both on the device and in some of its applications, indicating the location of a particular device; data—such as email, photos, videos, and messages—stored directly on a mobile device.[195]

Cognizant of the fact that their devices are potential gold mines of personal information, tech companies, including industry leaders Apple and Google, have joined the privacy debate.[196] As producers of "over ninety-six percent of the worldwide operating-system market share for smartphones," Google and Apple have struggled to protect their users' personal information from hackers.[197] Since 2014, versions of Apple's iOS and Google's Android have offered encryption capabilities,[198]

188 *See* CityBridge Franchise Agreement, *supra* note 5. For an updated map of Links across New York City, see https://www.link.nyc/find-a-link.html.

189 *See* CityBridge Privacy Policy, *supra* note 22.

190 *See id.*

191 *See* Burton W. King, *Castaway: Navigating Uncharted Waters*, 40 BROOK. J. INT'L L. 989, 990 (2015).

192 *See* Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 281 (2014).

193 "A smartphone is a mobile phone that offers personal computer functionality" . . . "[i]n addition to the ability to make calls and send and receive text messages." David Narkiewicz, *What Is A Smartphone and Why Do I Need One?*, 32 PA. LAW. 54, 54 (2010).

194 As of October 2014, 64% of adult Americans owning a smartphone, a figure that his since risen. *See* Finklea, *supra* note 162, at 1.

195 *Id.* at 3–4.

196 *See* John L. Potapchuk, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1404 (2016).

197 *Id.*

198 *Id.* Enabling encryption on both operating systems is simple. "Android's encryption feature

which experts have encouraged smartphone owners to use.[199] Apple claimed that its encryption was so secure under iOS 8 that even it was unable to access the encrypted data and was, therefore, unable to comply with government search warrants "even if . . . [it] wanted to."[200]

Apple stood by this claim in the face of Department of Justice (DOJ) search warrants and embarked on one of the most publicized instances of "corporate resistance"[201] in recent history. "Following the December 2, 2015 shooting in San Bernardino, California, investigators recovered a cell phone belonging to one of the suspected shooters."[202] The FBI was unable to unlock the cellphone,[203] leading the government to request an order under the All Writs Act directing Apple to bypass the iPhone's encryption.[204] Apple again refused to concede the application of the All Writs Act.[205] The court disagreed, ordering Apple to create and load Apple-signed software onto the iPhone that would disable its auto-erase function so that the government could examine the phone.[206] However, Apple's resistance was rendered moot, as the government was ultimately able to enter the iPhone with the help of a third-party.[207] However, the FBI indicated that the tool it used will not work on newer iPhone models.[208]

Undeterred by its unfavorable judgment in the San Bernardino Case, Apple continued its resistance to government pressure. This resistance culminated in the highly publicized decision, *In re Order*

requires a passcode entered into the phone every time it's powered back on." iOS users can encrypt their data just by enabling a passcode. iOS users may also set their phone to "delete all of its content if the passcode is entered incorrectly 10 times in a row." Roberto Baldwin, *Don't Be Silly. Lock Down and Encrypt Your Smartphone*, WIRED (Oct. 26, 2013), https://www.wired.com/2013/10/keep-your-smartphone-locked/.

199 *See* Baldwin, *supra* note 198.

200 *See* Finklea, *supra* note 162, at 5. Before iOS 8, "Apple maintained a 'key' that allowed the company to unlock any device without the passcode . . . . Apple had the ability to unlock devices for law enforcement . . . . [The key] was also vulnerable to exploitation by hackers, criminals, and others. iOS 8 enhanced automatic encryption and eliminated the back door key", thus preventing Apple from unlocking the encryption for anyone, even law enforcement." *See id.* at 6.

201 *See* Matt Apuzzo et al., *Apple and Other Tech Companies Tangle With U.S. Over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html (discussing the increased demand for built-in cellphone encryption modes available for encrypting digital communication and data stored on cellphones).

202 Finklea, *supra* note 162, at 9.

203 *See id.*

204 Matter of Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 2016 WL 618401, at *1 (C.D. Cal. 2016) (hereinafter The San Bernardino Case).

205 *Id.*

206 *See* Potapchuk, *supra* note 196, at 1406 n. 15 (citing The San Bernardino Case, 2016 WL 618401 at *1).

207 *Id.*

208 Devlin Barrett, *San Bernardino iPhone Hack Doesn't Work on Newer Models, FBI Says*, WALL STREET J. (Apr. 7, 2016), http://www.wsj.com/articles/san-bernardino-iphone-hack-doesnt-work-on-newer-models-fbi-director-says-1460050154.

*Requiring Apple, Inc. Assist in Execution of Search Warrant ("In re Apple, Inc.")*[209] where the government requested an order pursuant to the All Writs Act[210] to assist law enforcement agents in bypassing the iPhone's encryption in order to enable search of an iPhone. Apple refused to comply, and challenged the "courts' authority to compel the company to bypass its own encryption for the government."[211] Apple "argued that it no longer conceded that the All Writs Act" authorized this remedy.[212] In a landmark decision, Magistrate Judge Orenstein of The United States District Court for the Eastern District of New York held that All Writs Act did not authorize the remedy because "an order compelling Apple to provide unwilling technical assistance would not be 'agreeable to the usages and principles of law[.]'"[213]

Apple's ferocious opposition to the government, even in the face of a sharply divided public opinion[214] is encouraging for proponents of corporate resistance to government overreaching. Moreover, other companies, including Google, Facebook and WhatsApp have incorporated encryption into their products, signaling the increasing prominence of encryption.[215] Even though companies are beholden to their shareholders and, therefore, are not perfect proxies for the public, Apple's resistance gives us reason to believe that companies will in fact fight on behalf of the public. Whatever hope we have in that regard will entirely collapse if we allow this information to be freely handed over to the government. Unfortunately, the LinkNYC program may soon make this fear a reality.

This Note has argued that the LinkNYC program implicates state action. However, under the Court's current interpretation of the state-

---

209 *In re* Order Requiring Apple, Inc. Assist in the Execution of a Search Warrant, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (hereinafter In re Order Requiring Apple).

210 Potapchuk, *supra* note 196, at 1406 (citing 28 U.S.C. § 1651(a) (2012) (providing that "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."). From 2008 until Apple's resistance in 2015, the All Writs Act was an "investigative tool upon which . . . [the government] had routinely relied" to order companies to bypass encryption. *See* Potapchuk, *supra* note 196, at 1403.

211 *See* Potapchuk, *supra* note 196, at 1403.

212 *See* Potapchuk, *supra* note 196, at 1406.

213 *See* Potapchuk, *supra* note 196, at 1432 (citing *In re Order Requiring Apple*, 149 F. Supp. 3d at 349, 363–64).

214 By some estimates, a majority of the public wanted Apple to unlock the iPhone in the San Bernardino Case. *See More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone*, PEW RES. CTR. (Feb. 22, 2016), http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/. However, many took an opposing view. *See, e.g.*, Ken Gude, *The FBI Is Dead Wrong: Apple's Encryption Is Clearly in the Public Interest*, WIRED, Oct. 17, 2014, https://www.wired.com/2014/10/fbi-is-wrong-apple-encryption-is-good/.

215 Joseph Menn & Julia Love, *Apple's War with the FBI Could Speed up the Development of Government-Proof Tech*, BUS. INSIDER (Feb. 24, 2016, 7:02 AM), http://www.businessinsider.com/r-apples-fight-with-us-could-speed-development-of-government-proof-devices-2016-2.

action doctrine, it is unclear whether this result would occur.[216] If the court were to find that the state-action doctrine is not implicated, a perverse result would occur. This would result in a scenario in which a municipality could escape Fourth Amendment scrutiny for information that it collects by operating through a nominal third party. As Jeremy H. D'Amico stated, "[i]t seems disingenuous for the government to require a third party to monitor the location of cellphones and then to use the third-party doctrine to request the records that the government compels the third party to create in the first place."[217] It seems just as disingenuous for the City of New York to require LinkNYC to amass a wealth of data just to use the third-party doctrine to obtain that same information.

## IV. THE FUTURE OF LINKNYC

As discussed, though the LinkNYC program implicates the state-action doctrine, a court would likely determine that a user has no reasonable expectation of privacy in the data collected by the LinkNYC program based on the third-party doctrine.[218] Without the protections of the Fourth Amendment, the only protection that users of the LinkNYC program enjoy is the privacy policy signed by the City of New York and CityBridge.[219] However, given the immense personal information that the program handles every day, contractual protection is insufficient.

It is easy to imagine a future catastrophic event that would convince the city or state governments to rewrite the existing privacy policy in order to collect more information in aid of potential police investigations. Such "crisis legislation"[220] is not hard to imagine since "[f]ollowing major disasters that provoke fear, sadness, or anger, citizens demand action from their legislators and, in their haste, 'are too focused on the emergency . . . to protect their interests.'"[221] After all, this is precisely what happened in in the wake of the terrorist attacks of September 11, 2001 ("9/11").[222] The USA PATRIOT Act of 2001[223] was a response to the attack and was designed to loosen

---

216 See discussion *supra* Section I.B.

217 Jeremy H. D'Amico, *Cellphones, Stingrays, and Searches! An Inquiry into the Legality of Cellular Location Information*, 70 U. MIAMI L. REV. 1252, 1286–87 (2016).

218 See discussion *supra* Section I.C.

219 *See* Hirose, *supra* note 24, at 1.

220 Kyle Welch, *The Patriot Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking*, 43 CAP. U. L. REV. 481, 481 (2015) (arguing that incidents of fearful congressional overreaction should be properly labeled as "crisis legislation").

221 *Id.* at 482 (internal citations omitted).

222 On September 11, 2001, the United States suffered a series of coordinated terrorist attacks in which nearly 3,000 Americans lost their lives. *See id.* at 485–86.

223 USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered U.S.C. titles 8, 12, 15, 18, 20, 31, 42, 47, 49, and 50) [hereinafter Patriot Act].

perceived restraints on obtaining information about suspected terrorists and future attacks.[224] The general public is now collectively willing to, in moments of fear, cede protections of its rights in exchange for a fleeting sense of security. The agreements governing LinkNYC's use are not adequate protection, as they, like all contracts, can be amended.

However, one need not contemplate such a dire situation to demonstrate the inadequacy of LinkNYC's contractual protection. It is entirely reasonable to believe that CityBridge and the City of New York will renegotiate their governing agreements at some point in the future. It is further plausible that the City will follow in the footsteps of Google who has explicitly admitted to scanning communications for content for advertising purposes.[225]

It may appear that the Electronic Communications Privacy Act of 1986 ("ECPA")[226] is a quick answer to both hypotheticals. However, the ECPA has several exceptions that would preclude its application in the context of LinkNYC.[227] By employing either the Consent or Provider Exception, LinkNYC and the City of New York would be able to skirt the protections of the ECPA, and leave users unprotected. In order to adequately protect users of municipal Wi-Fi programs, it is clear that Congress must amend the ECPA to explicitly preclude the application of the Consent and Provider Exceptions in the context of municipal Wi-Fi programs. This Note proposes that Congress amend § 2511(2)(d) [The Consent Exception] and § 2511(2)(a)(i) [The Provider Exception] of the ECPA to explicitly preclude their application in the context of municipal Wi-Fi programs.

---

[224] John T. Soma et. al., *Balance of Privacy vs. Security: A Historical Perspective of the USA Patriot Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285 (2005) (citing USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[225] *See* Matera v. Google, 2016 WL 5339806 (N.D. Cal. 2016).

[226] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (hereinafter the "ECPA"). "The body of electronic surveillance laws created by the ECPA breaks down into three statutes: the Wiretap Act, . . . the Pen Register statute, . . . and the Stored Communications Act." Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004). The ECPA amended Title III of the 1968 Omnibus Crime Control and Safe Streets Act (the "Wiretap Act"), which itself was primarily designed to prevent unauthorized government access to private electronic communications, in order to make it more applicable to modern, digital communications. *See id.* at 1566. The Wiretap Act, and its exceptions, will be the focus of the remainder of this Note.

[227] *See* 18 U.S.C. §§ 2511(2)(d), 2511(2)(a)(i). The Patriot Act amended the ECPA in several ways. First, it changed the definition of "wire communication" to eliminate electronic storage from the definition of wire communication. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 n.8 (3d Cir. 2003), *as amended* (Jan. 20, 2004). Additionally, commentators have noted that the Wiretap Act has a robust exclusionary rule, "as any information obtained through an unlawfully intercepted communication may not be offered as evidence in any trial." Peter Murphy, *An Examination of the United States Department of Justice's Attempt to Conduct Warrantless Monitoring of Computer Networks Through the Consent Exception to the Wiretap Act*, 34 CONN. L. REV. 1317, 1321–22 (2002).

### A. *The "Consent Exception"*

The ECPA contains a consent exception that permits one party to an electronic communication to give prior consent to interception.[228] "[The enactment of the consent] exception reflect[ed] a line of cases, decided under the Fourth Amendment, allowing recording or eavesdropping by government agents or informers who were parties to the conversation or who were allowed to listen by explicit consent of a party to the conversation."[229] The exception has been interpreted to require knowing assent to monitoring.[230]

A recent United States Department of Justice ("DOJ") manual is instructive in understanding the sweeping application of the consent exception.[231] The DOJ indicated in its most recent manual on the investigation of computer crimes that the consent exception to the Wiretap Act applies in computer cases if the network has been properly equipped with a network banner:[232] "For purposes of warrantless monitoring by the government, the banner would have to include language that informed users that their use may be monitored, and that subsequent use of the system would constitute consent to the monitoring."[233]

Applying the DOJ manual to the case of LinkNYC, the City of New York and CityBridge could draft new software that includes a network banner with an adequate warning to avoid the scrutiny of the ECPA. Additionally, the Consent Exception to Title III could also be implicated in the context of consenting for advertising purposes. Provided that the City and CityBridge obtain consent, they may enjoy the application of the Consent Exception as it currently stands.

---

[228] *See* 18 U.S.C. § 2511(2)(d) (2012) "It shall not be unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act . . . ." *See also,* Ariana R. Levinson, *Toward A Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461 (2012).

[229] *See* Murphy, *supra* note 227, at 1323.

[230] *See* Levinson, *supra* note 227, at 494 (citing Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 819 (N.D. Ill. 1981)).

[231] *See* Murphy, *supra* note 227, at 1320 (citing U.S. Dep't Of Justice, Searching And Seizing Computers And Obtaining Electronic Evidence In Criminal Investigations, ch. 4, pt. C(3)(b) (2001) [hereinafter Searching & Seizing Computers], at http://www.cybercrime.gov/searchmanual.htm.

[232] *Id.* "Network banners are electronic messages or signs that provide notice of legal rights to users of computer networks." *Id.* at 1330.

[233] *Id.* at 1330.

### B. *The "Provider" Exception*

CityBridge may also seek to make use of the ECPA's "Provider" Exception.[234] The Provider Exception allows a communications service provider "to intercept, disclose, or use [a] communication in the normal course of [its] employment while engaged in any activity which is a necessary incident to the rendition of [its] service or to the protection of the rights or property of the provider of that service."[235]

Pursuant to the Franchise Agreement governing the operation of the LinkNYC program, CityBridge has the authority to operate the wireless network.[236] Courts differ in their application of the Provider Exception,[237] with some courts interpreting the language to exempt a provider under any circumstances.[238] A court applying the broad reading of the Provider Exception would likely hold that CityBridge and the City of New York are exempt from the protection of the Wiretap Act given their status as Service Providers.

### C. *Amending the ECPA To Limit the Consent and Provider Exceptions*

The preceding discussion demonstrates that the ECPA does not adequately protect LinkNYC user privacy. By employing either the Consent or Provider Exceptions, LinkNYC and the City of New York would be able to skirt the protections of the ECPA, and leave users unprotected. This is especially worrisome given that the LinkNYC Program is providing an essential service for a segment of New York City's population.[239] Municipalities must not be permitted to force citizens to sacrifice privacy through implied consent to an adhesion contract. Given these concerns, it is clear that Congress must amend the ECPA to explicitly preclude the application of the Consent and Provider

---

234 18 U.S.C. § §2511(2)(a)(i) (The Provider exception permits: "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.").

235 Matthew A. Chivvis, *Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 799, 808 (2009).

236 *See* CityBridge Franchise Agreement, *supra* note 5.

237 *See, e.g.*, Levinson, *supra* note 230, at 502–03.

238 *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003) (holding that the service provider exception exempts from the SCA's "protection all searches by communications service providers.").

239 *See supra* notes 94–102 and accompanying text.

Exceptions in the context of municipal Wi-Fi programs. Therefore, Congress should amend § 2511(2)(d) [The Consent Exception] and § 2511(2)(a)(i) [The Provider Exception] to explicitly preclude their application in the context of municipal Wi-Fi programs.

Critics of this position will argue that limiting the ECPA's exceptions in this manner runs counter to the American ideal of freedom of contract, and well-established Supreme Court precedent.[240] However, proposals regarding ECPA and freedom of contract are within the context of employment law[241] and can be distinguished on those grounds alone. Moreover, those seeking amend the Wiretap Act in a way that preserves the Consent Exception have proposed more robust prerequisites to invoking the Consent exception, like obtaining express written consent followed by oral consent of the user.[242] While these suggestions may be plausible in the context of employment law, they are unrealistic in the context of municipal Wi-Fi programs, as obtaining express written and oral consent from each LinkNYC user is unrealistic, not only because of the vast number of Users, but also because some users likely may not entirely understand what they are assenting to.[243] Additionally, employees using employer-provided servers are charged with a level of sophistication that may not be attributed to the general public.

Though Congress intended that consent under the ECPA may be implied,[244] municipal Wi-Fi programs must not be permitted to rely on implied consent from unsophisticated Users of the LinkNYC program. Indeed, courts have only been willing to imply consent in limited circumstances.[245] Cases in which the courts have found implied consent have been based on facts that "illustrate that the person monitored knew the monitoring was taking place and assented to it."[246] Such an illustration will be not possible in all cases in the context of LinkNYC, as many Users are likely to lack the sophistication to meaningfully assent to such monitoring.[247] Moreover, courts are willing to consider inequity of bargaining power in assessing the presence of implied consent.[248] Conducting such an inquiry in this case illustrates the gross inequity in bargaining power between the City of New York and Users

[240] *See* Chivvis, *supra* note 235, at 824 n. 169 (arguing that Lochner v. New York, 198 U.S. 45, 57 (1906), where the Supreme Court struck down a precursor to the Fair Labor Standards Act, unconstitutionally interfered with the right of contract between the employer and employees.)
[241] *See* Chivvis, *supra* note 235, at 825; Levinson, *supra* note 228, at 529.
[242] *See* Chivvis, *supra* note 235, at 827–28.
[243] *See* Menschel, *supra* note 7, at 149–50.
[244] *See* Levinson, *supra* note 230, at 496 (citing S. REP. NO. 90-1097 (1968), which provided for implied consent).
[245] *See* Levinson, *supra* note 230, at 497.
[246] *Id.* at 497 n. 204.
[247] *See* Menschel, *supra* note 7, at 149.
[248] *See* Levinson, *supra* note 230, at 496 n. 200.

of LinkNYC, and the need for the Consent and Provider Exceptions to be limited in the context of municipal Wi-Fi.

However, removing only the Consent Exception while preserving the Provider Exception in the context of municipal Wi-Fi is not sufficient to protect users' privacy interests on its own, as some courts read the Provider Exception to exempt a provider from the ECPA under any circumstance.[249] Moreover, abandoning the Consent and Provider Exceptions in the context of municipal Wi-Fi is not as drastic as it may seem, since some Courts have refused to apply them strictly in their current form.[250]

Moreover, amending the ECPA to remove the Consent and Provider exceptions in the context of municipal Wi-Fi is consistent with Congress' stated intent surrounding the passage of the ECPA.[251] Both the House and Senate expressed concern of the pervasiveness of technology[252] and wanted to create a legislative solution that could stand up to increasingly more sophisticated technology.[253]

Most of all, the elimination of the Consent and Provider Exceptions in the context of municipal Wi-Fi programs is consistent with positions expressed by the Court in *United States v. Jones*, in which Justice Sotomayor questioned whether the historic notions of consent that underlie the third-party doctrine should be applicable in the digital age.[254] Voluntary use of a municipal Wi-Fi program "should not, for that reason alone, disentitle[ ] [a user] to Fourth Amendment protection"[255] any more than it should also not disentitle a user to protection under the ECPA. In light of this conclusion, the ECPA should be amended by Congress or read by the courts to be applicable, without exception in the context of Municipal Wi-Fi programs like LinkNYC.

## V. CONCLUSION

Although the LinkNYC program likely falls within the state-action doctrine and therefore triggers the protections of the Fourth Amendment, it is unlikely that a LinkNYC User would have any reasonable expectation to privacy while using the program under the Supreme Court's antiquated third-party Doctrine. The third-party

[249] *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003); *see also* Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 144 (2005).
[250] *See* Hornung, *supra* note 249, at 144.
[251] *See* Levinson, *supra* note 228, at 480.
[252] *See id.* at 481–82.
[253] *See id.* at 482.
[254] *See* U.S. v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
[255] *Id.*

doctrine as it stands today has thus created a scenario in which a municipality is able to escape Fourth Amendment scrutiny for information that it collects by operating through a nominal third party. The fact that the LinkNYC program provides an essential service for a segment of the population amplifies the perverse results of this situation by creating the potential for a two-tiered system of privacy rights in which rich New Yorkers are subject to different privacy policies than are poor New Yorkers. The Internet is a necessity, and some poor citizens cannot use it anywhere else. In this situation, poorer citizens who have no choice but to use the city-sponsored Wi-Fi will be subject to different privacy standards than wealthier residents who contracted with a private Internet Service Provider. Moreover, the existing privacy policy governing the LinkNYC program is insufficient to protect these interests. Given these risks, the ECPA should be amended by Congress or read by the courts to be applicable, without exception in the context of Municipal Wi-Fi programs like LinkNYC.

*David Forrest*[*]

[*] Notes Editor, CARDOZO ARTS & ENT. L.J. Vol. 36, J.D. Candidate, Benjamin N. Cardozo School of Law (2018); B.A., Political Science, Binghamton University (2015). I would like to thank Professor Ekow Yankah for his insight and guidance throughout the development of this Note. I would also like to thank the members of AELJ Vol. 35 & 36 for their editorial contributions to this Note. Finally, I would like to thank my family for their unwavering patience and support throughout my law school journey.