SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

In re Application for a Judgment under Article 78 of the Civil Practice Law and Rules by SUSAN CRAWFORD, Petitioner, -against- NEW YORK CITY DEPARTMENT OF INFORMATION TECHNOLOGY TELECOMMUNICATIONS, Respondent, AND AT&T CORP., EMPIRE CITY SUBWAY COMPANY LTD., TIME WARNER CABLE INC., and RCN TELECOM SERVICES, LLC., Intervenors-Respondents.	Index No. 157002/2015 IAS Part 6 (Lobis, J.)

JOINT MEMORANDUM OF LAW OF INTERVENOR-RESPONDENTS AT&T, TWC, AND RCN IN OPPOSITION TO THE ARTICLE 78 PETITION

Craig R. Bucki, Esq.
Phillips Lytle LLP
The New York Times Building
620 Eighth Avenue, 23rd Floor
New York, New York 10018

Hans J. Germann
Mayer Brown LLP
71 S. Wacker Drive
Chicago, IL 60606
Attorneys for Intervenor-Respondent AT&T Corp.

Douglass B. Maynard, Esq.
Jessica Oliff Daly, Esq.
Akin Gump Strauss Hauer & Feld LLP
One Bryant Park
New York, NY 10036
Attorneys for Intervenor-Respondent Time Warner Cable Inc.

Thomas M. Smith, Esq.
Eckert Seamans Cherin & Mellott, LLC
10 Bank Street, Suite 700
White Plains, NY 10606
Attorneys for Intervenor-Respondent RCN Telecom Services, LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Preliminary Statement

Intervenor-Respondents AT&T Corp. ("AT&T"), Time Warner Cable Inc. ("TWC"), and RCN Telecom Services, LLC ("RCN") (collectively, "Intervenors") hereby jointly submit this memorandum of law in opposition to the Petition brought by Susan Crawford ("Petitioner") pursuant to Article 78 of the New York Civil Practice Law and Rules ("CPLR").

Under New York Public Officers Law § 84 *et seq.* (the "Freedom of Information Law" or "FOIL"), Petitioner seeks disclosure from the New York City Department of Information Technology and Telecommunications ("DoITT") of information showing the exact location and use of underground conduit owned by ECS, which supports telecommunications networks in New York City. AT&T, TWC, and RCN are telephone, video, and Internet communications providers and tenants of ECS, and some of the information sought by Petitioner concerns their facilities. Intervenors oppose the Article 78 Petition because public release of the information sought by Petitioner would threaten the security of Intervenors' facilities, endanger public safety, and substantially injure the competitive positions of the Intervenors by revealing confidential and proprietary information about their facilities.

The information at issue consists of an ECS spreadsheet, which ECS provided to DoITT, identifying each ECS conduit, the locations of the manholes at the endpoints of each conduit, the identity of the tenant(s) occupying each conduit run, and the ducts and number of ducts occupied by the tenant(s) in each conduit run. While each of the Intervenors is familiar with the precise location and extent of its own facilities within ECS conduit, they do not have that same information about one another's facilities. Rather, the Intervenors have seen only the same redacted version of the spreadsheet at issue as was provided to Petitioner. The unredacted information is not made available to the Intervenors or more generally to the public, and for good reasons.

First, disclosure of the information at issue would threaten the security of the telecommunications network because it includes sensitive information about the location and use of telecommunications facilities in the ECS system. As the Court stated in denying Petitioner's previous Article 78 Petition seeking information about the ECS conduit system, there is a "real life danger" that "the release of sensitive information . . . may result in an attack on our information technology assets." *Matter of Crawford v. N.Y. City Dep't of Info. Tech. & Telecomms.*, 43 Misc. 3d 735, 743 (Sup. Ct. N.Y. Cty. 2014). DoITT therefore properly denied Petitioner's FOIL request because the information at issue is within the scope of the "information technology exemption" to FOIL, which protects information whose disclosure would jeopardize the security of "information technology assets," including "infrastructures." N.Y. PUB. OFF. LAW § 87(2)(i).

Second, for similar reasons, the information at issue is exempt from disclosure because its disclosure "would endanger the life or safety of any person." N.Y. PUB. OFF. LAW § 87(2)(f).

Third, the Intervenors' information also constitutes trade secrets that Intervenors routinely treat as confidential and proprietary. Disclosure of this information would substantially harm the Intervenors' competitive positions because it would reveal information about their strategic network builds, which they have expended substantial resources in developing and marketing. Were that information to be disclosed to competitors, they could exploit it to the Intervenors' competitive disadvantage through tactical decisions regarding network and resource allocation and solicitation of their customers. DoITT therefore properly denied Petitioner's FOIL request because the information at issue is within the scope of the "trade secret exemption" to FOIL, which protects both "trade secrets" and information submitted to an agency by a

commercial enterprise "which if disclosed would cause substantial injury to the competitive position" of the enterprise. N.Y. PUB. OFF. LAW § 87(2)(d).

Intervenors therefore request that the Court deny the Article 78 Petition.

Background

Since 1891, ECS has held a franchise from the City of New York ("the City") to build and maintain a conduit and manhole infrastructure in the City. NYSCEF Dkt. No. 12, Affidavit of Robert F. Connolly, sworn to on Nov. 6, 2015 ("Connolly Aff.") ¶ 4. ECS owns approximately 58 million feet of conduit and 11,000 manholes. *Id.* ECS leases space in conduits to various telecommunications and cable television service providers, including the Intervenors. *Id.*

DoITT is an agency that administers the franchise agreement between the City and ECS and oversees ECS within its franchise area. *Id.* ¶ 5. Based on DoITT's oversight authority, ECS must produce documents, data and other information relating to ECS's business operations and tenants on a regular basis. *Id.* Prior to turning over its documents to DoITT, ECS engages in a rigorous analysis to determine whether the information contained is sensitive, confidential and proprietary. *Id.* If it is, ECS clearly denotes this on the document produced, and asserts statutory rights under FOIL to prevent disclosure of the information to third parties. *Id.*

On May 9, 2014, Petitioner made a FOIL request seeking, among other things, records "concerning DoITT's regulation of any Internet infrastructure owned or operated by Empire City Subway Company Ltd." Verified Petition, NYSCEF Dkt. No. 1 ("Pet."), Ex. A at ¶ 1. DoITT provided a partial response to Petitioner's request on November 21, 2014. *Id.* ¶ 12. On January 30, 2015, DoITT completed its response to Petitioner and disclosed a redacted version of a spreadsheet prepared by ECS (the "Spreadsheet"). *Id.* ¶ 14. Before producing the Spreadsheet to Petitioner, DoITT redacted entries that describe the locations of manholes and

conduits owned or maintained by ECS and entries that identify tenants who occupy those conduits. Connelly Aff. ¶ 9.

When ECS submitted the Spreadsheet to DoITT, it conspicuously stated on the Spreadsheet the following language:

> This document contains confidential and competitively sensitive information of both Empire City Subway and its tenants. Empire City Subway requests that this information be treated as confidential and proprietary, and that, in accordance with Public Officers Law § 87(2)(d) and 87(2)(f), it not be disclosed. This information is not otherwise readily ascertainable or publicly available by proper means by other persons from another source in the same configuration as provided herein, would cause substantial harm to the competitive position of Empire City Subway (and its tenants) if disclosed, is intended to be proprietary confidential business information, and is treated by Empire City Subway as such. Disclosure of the information would also constitute a security risk as it could endanger the life or safety of New York City residents and visitors.

Id. ¶ 8.

DoITT refused to disclose the redacted information, asserting it was exempt from disclosure under FOIL. Pet. ¶¶ 14-15. On February 26, 2015, Petitioner submitted an administrative appeal to DoITT challenging the redactions. *Id.* ¶ 16. On March 12, 2015, DoITT granted in part and denied in part Petitioner's administrative appeal. *Id.* ¶ 17. DoITT provided the names of ECS's tenants, but did not disclose the location of the tenants' conduits. *Id.* On July 10, 2015, Petitioner commenced this proceeding seeking an unredacted version of the sensitive, confidential and proprietary information contained in the Spreadsheet. On April 15, 2016, the Court granted the petitions to intervene of AT&T, ECS, TWC,[1] and RCN. NYSCEF Doc. No. 119.

[1] TWC was merged out of existence in May 2016. Charter Communications, Inc. and its subsidiaries, directly or indirectly now own the assets formerly held by TWC.

Argument

I. The Requested Information Falls Within The Information Technology Disclosure Exemption Because Its Release Would Threaten The Safety Of The Communications Network.

FOIL permits an agency to deny access to records that "if disclosed, would jeopardize the capacity of an agency or an entity that has shared information with an agency to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures." N.Y. PUB. OFF. LAW § 87(2)(i).

In the prior *Crawford* proceeding, the Court held that this "information technology exemption" applies to maps showing the specific locations of ECS's underground conduits. *Matter of Crawford v. N.Y. City Dep't of Info. Tech. & Telecomms.*, 43 Misc. 3d 735, 740-43 (Sup. Ct. N.Y. Cty. 2014). In reaching this conclusion, the Court rejected Petitioner's suggestion that the information technology exemption is limited to risks of electronic "cyber" attacks on information technology assets. *Id.* at 740-41. Rather, the Court found that the information technology exemption also includes risks of physical attacks on information technology infrastructure, including ECS's conduits, because "[t]his security consideration is not merely focused on the method of attack, but on the preservation of both electronic data and the physical system or infrastructure that carries the data." *Id.* at 741.

The Court then concluded that the City had demonstrated that "the release of the precise location of the conduits would make our fiber optic network more susceptible to terrorist or other attack." *Crawford*, 43 Misc. 3d at 743. The maps that were at issue "show the fiber optic network in great detail," which network carries "voice and data transmissions and provide[s] internet and phone access throughout New York City." *Id.* at 742. "Both the private and government sector," including "the banking and financial communities" and "the New York

City, State and federal courthouses, emergency communications call centers, hospitals, police and fire departments," "heavily rely on the fiber optic network to conduct their affairs." *Id.*

Petitioner attempts to distinguish her prior case by arguing that the data at issue here does not identify conduit pathways into and out of "high risk" targets like banks and government buildings, but rather, "identifies conduits flowing through specific *manholes only*." Pet'r's Mem. at 12 (emphasis in original). But the security concerns driving the Court's understanding of the information technology exception in the prior *Crawford* case were not limited to the risks posed to individual high-profile targets on the communications network. Rather, the communications network *itself* is a high-profile target. Thus, the Court noted that a "precisely targeted attack on certain cables 'could result in an internet disruption not only in New York City but also throughout the United States and overseas.'" *Crawford*, 43 Misc. 3d at 742. The Court also noted that "release of the precise location of the conduits would make our fiber optic network more susceptible to terrorist or other attack." *Id.* at 743. Such concerns are in keeping with the language of the FOIL exemption itself, which does not focus only on the security of particular users of information technologies, but more broadly protects information that would jeopardize the security of "information technology assets," including "infrastructures."

Petitioner also argues that the data at issue here does not fall under the information technology exemption because it does not consist of maps, but rather of a spreadsheet identifying each ECS conduit, the locations of the manholes at the endpoints of each conduit, the identity of the tenant(s) occupying the conduit run, and the ducts and number of ducts occupied by the tenant(s) in each conduit run. Petitioner is wrong, because this data is every bit as sensitive as

maps showing the routes of these conduit runs, and indeed would allow a person to build a virtual topographical map of all the service providers within the ECS system.[2]

As explained in the Affidavits of Christopher F. McDermott (sworn to on January 31, 2017, and submitted on behalf of AT&T ("McDermott Aff.")), and Noel Dempsey (previously submitted at NYSCEF Dkt. No. 18, sworn to on Nov. 11, 2015, and submitted on behalf of TWC ("Dempsey Aff.")), a person intent on causing harm could use the unredacted information requested by Petitioner to maximize disruption to communications and data throughout the City.[3] Manholes are, by definition, natural points of access to conduits and communications cables (as opposed to, *e.g.*, digging up the streets to access the middle of a conduit run), and hence are the most likely targets for persons intent on disrupting communications networks.

In 2014, an advisory council of the Federal Communications Commission ("FCC") asked a panel of industry experts to investigate the security of manholes.[4] According to the FCC, this "high priority issue" was "directly related to vandals inappropriately accessing manholes and damaging communications facilities." *Id.* The industry experts' report asserted that the nation's communications infrastructures are "mission critical circuits for consumers, government and communication providers" and that for "bad actors that are determined to cause a disruption to communications or emergency services the unremarkable and often unobtrusive manhole cover is the equivalent of an unlocked door." *Id.* The final report from the experts acknowledged the many security risks posed by unfettered access to manhole covers and the cables they connect. *Id.*

---

[2] For this reason, as DoITT previously asserted, the doctrine of *res judicata* bars the Petition because the unredacted spreadsheet provides the same information as the maps sought in *Crawford I*. NYSCEF Doc. No. 53.

[3] Intervenors also submit herewith affidavits from Sprint, Optical Communications, Altice/Cablevision, and Axiom Fiber Networks, all tenants of the ECS system, who similarly explain that disclosure of their network information would jeopardize the security of their networks.

[4] *See* COMMUNICATIONS SECURITY, RELIABILITY AND INTEROPERABILITY COUNCIL, WORKING GROUP 7, "LEGACY BEST PRACTICES UPDATE, INTERIM REPORT – MANHOLE SECURITY" (March 2014) (Exhibit A to the February 3, 2017 Affidavit of Craig R. Bucki ("Bucki Aff.")).

Further, the information at issue would, among other things, allow a person to identify the specific locations of particular manholes containing large numbers of occupied conduits, relied upon by a large number of carriers. For instance, the second page of Petition Exhibit G identifies certain routes that contain very high numbers of in-use conduits, compared to other conduit runs shown. The redacted information on the first page of that Exhibit would allow a person to identify every ECS tenant with facilities accessible at these two manhole locations. This could include carriers (such as AT&T and Sprint), government users (such as the Unified Court System, the Federal Reserve, NYPD, and NYFD), and educational institutions (such as Columbia University). Manholes containing a large number of conduits, or conduits servicing high-profile users, could in this way be identified and targeted to maximize communications outages and havoc. *See* McDermott Aff. ¶ 8.

The communications cables in these conduits are used to serve all kinds of communications needs, including voice, Internet, and other data services provided to individuals, businesses, financial institutions, educational and other organizations, and Federal, State, and local governments and agencies. The voice traffic carried over the Intervenors' facilities includes emergency communications, such as 911 calls. It also includes wireless traffic, as most wireless traffic is actually carried by wireline cable for a portion of its transmission to and from cell towers. All of these communications could be significantly disrupted, for a prolonged period, by a strategic attack on heavily used conduit routes. McDermott Aff. ¶ 5; *see also* Affidavit of Brian J. Allen, sworn to on Nov. 11, 2015 ("Allen Aff.") ¶¶ 4-12 (explaining the critical nature of the services provided by TWC).

Similarly, individual high-profile targets could be put at increased risk by public release of the data at issue. For example, a person seeking to target a particular communications

provider could use the requested information to identify main trunk lines and points of network aggregation where large numbers of facilities converge. Further, by identifying which particular manholes do and do not contain 'active' conduit and which are used or are not used by particular providers, the data could confirm or refute the presumption that manholes adjacent to a target contain conduit servicing that building. In addition, a person intent on disrupting communications to a high-profile target could use the data to evade surveillance cameras and other security measures at that location by tracing a conduit route to identify possible access points blocks away from the target, or even further if multiple conduit segments were traced. *See* McDermott Aff. ¶ 10; Dempsey Aff. ¶¶ 8-9.

Petitioner also argues that any security concerns regarding public release of the requested information are entirely speculative. Petitioner's argument is demonstrably wrong, because communications networks have already been the targets of attacks by vandals or others seeking to destroy communications infrastructure and/or cause widespread communications outages. For example, in the past few years, a person or persons have on multiple occasions done just that in the Bay Area in California. Among other incidents, in April 2009, vandals cut underground fiber optic cables in four manholes, knocking out landlines, cell phones and Internet service for tens of thousands of people in Santa Clara, Santa Cruz and San Benito counties. In April 2013, simultaneous with a sniper attack on an electric substation, nearby manholes were accessed and fiber optic cables cut, resulting in significant outages. In July 2014, five manholes were breached in the Bay Area and fiber cables belonging to seven providers were cut. In June 2015, three manholes were breached within hours of one another and multiple providers' fiber optic cables were cut. *See* McDermott Aff.¶ 11.

Several recent news articles also highlight the vulnerability of infrastructure like the ECS conduit network and demonstrate experts' concerns that the network could be targeted. In November 2015, the New York Times published an article entitled "The Cyberthreat Under the Street" which focused on the safety risks created by access to underground cables.[5] According to the article, damage could be inflicted on "Internet exchange points" or "I.X.Ps" which could cause data transfer to slow significantly or come to a halt. *Id.* The article also reported that one academic recently completed a map of the United States' long-haul internet infrastructure and that the map can only be accessed by Department of Homeland Security-approved researchers because of concerns about what could be done if the information was made available to the public. *Id.* Another article reported in 2013 that a nexus of underwater cables off the coast of Egypt had been attacked.[6] The article indicated that the attack may have been an effort by a terrorist group to cut off Internet communications to that country. *Id.*

Additionally, in October 2015, the New York Times reported that American military and intelligence officials are concerned about activities by Russian submarines near the undersea cables that carry global Internet communications.[7] The officials fear that Russian forces might attack those lines in times of tension or conflict. *Id.* The article noted that the role of the undersea cables "is more important than ever before" as they carry trillions of dollars worth of global business from financial institutions that settle transactions every second. *Id.* Any significant disruption in the cables would cut that global flow of capital. *Id.* Given New York's position as one of the centers of global finance, it is reasonable to hypothesize that an attack on New York

---

[5] Kate Murphy, *The Cyberthreat Under the Street*, N.Y. TIMES (Nov. 7, 2015) http://www.nytimes.com/2015/11/08/sunday-review/the-cyberthreat-under-the-street.html?smid=nytnow-share&smprod=nytnow&_r=0 (Bucki Aff. Ex. B).

[6] David Shamah, *Internet cable-cutters caught by Egypt signal new terror threat*, TIMES OF ISRAEL, (Mar. 29, 2013) http://www.timesofisrael.com/internet-cable-cutters-caught-by-egypt-signal-new-terror-threat/ (Bucki Aff. Ex. C).

[7] David E. Sanger and Eric Schmitt, *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, N.Y. TIMES (Oct. 25, 2015) http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html (Bucki Aff. Ex. D).

City's cable network might be equally attractive to those wanting to disrupt global Internet communications during times of tension or conflict.

The Federal Communications Commission ("FCC") and other authorities have consistently found that information regarding the specific routes and locations of communications networks should be kept confidential in light of security concerns. For example, in *In re Special Access for Price Cap Local Exchange Carriers*, 29 FCC Rcd. 11657, 2014 WL 4964597, ¶ 10 (FCC 2014), the FCC adopted protective measures to prevent the public disclosure of "information on network maps and locations served that if disclosed could compromise network security." Similarly, in a 2013 report the FCC acknowledged significant confidentiality concerns related to sharing "proprietary information about a service provider's specific network architecture or operations on a less than aggregated basis," and stated that it would treat as "presumptively confidential and exempt from routine public disclosure under the Freedom of Information Act" information such as "circuit routes and diagrams." *In the Matter of Improving 911 Reliability*, PS Docket No. 13-74, 11-60 (FCC 2013) (Bucki Aff. Ex. F). *See also, e.g., In the Matter of Centurylink Qcs Serv. Quality & Its Response to Notice of Comm'n*, 2015 WL 2090211, at *3 (Mont. Pub. Serv. Comm'n 2015) ("the Commission agrees that due to network security concerns, all location information should be redacted from the public version of Exhibit 5," showing the location of telecommunications provider's facilities); *In re Verizon Del. Inc.*, 2006 WL 4748770 (Del. Pub. Serv. Comm'n 2006) ("In these post-September 11, 2001 times, there can indeed be significant and legitimate security concerns about whether information related to the operation and location of telecommunications networks should be publicly available from State agencies."); *Tel. Ass'n of Me. Request for Protective Order for Info. on Page*

27 of Annual Report, 1999 WL 35368087 (Me. Pub. Utils. Comm'n 1999) (concluding that interoffice network configuration information should be non-public due to security concerns).

In short, a person attempting to substantially disrupt communications in New York City, whether for purposes of terrorism, vandalism, or other criminal purposes, would be greatly assisted by access to the information that Petitioner seeks to make publicly available. Public release of the information redacted by DoITT would allow those intent on causing harm to identify "high value" targets to compromise public safety, interfere with emergency and first responder communications, substantially disrupt all other communications (including voice, data, and Internet services) throughout the City and beyond, and throw the financial and banking communities into disarray. As the New York Public Service Commission stated, "September 11th 2001 redefined 'telecommunications disaster' and underscored the importance of the public telecommunications network. Telecommunications network reliability, increasingly viewed through a prism of national security and public safety considerations, is no longer a luxury, but a political and economic mandate." *In re Motion of Comm'n to Examine Issues Related to Transition to Intermodal Competition in Provision of Telecomms. Servs.*, 248 P.U.R.4th 71 (N.Y.P.S.C. 2006). Granting Petitioner's request would threaten that mandate and jeopardize the reliability of the City's communications network. *Cf. Crawford*, 43 Misc. 3d at 743 ("While the unforgettable attack on the World Trade Center towers seems not to have been anticipated, we are now all much more vigilant to guard against the same, new or different terrorist attacks.").

II. Disclosure of the Conduit Location Information Would Endanger Life and Public Safety.

FOIL also permits an agency to deny access to records that, "if disclosed, would endanger the life or safety of any person." N.Y. PUB. OFF. LAW § 87(2)(f). This exemption also applies to the Spreadsheet.

In order to rely on this "life or safety" FOIL exemption, an agency need only demonstrate "a possibility of endangerment." *Matter of Bellamy v. N.Y. City Police Dep't*, 87 A.D.3d 874, 875 (1st Dep't 2011) aff'd, 20 N.Y.3d 1028 (2013) (internal quotations omitted); *see also Asian Am. Legal Def. & Educ. Fund*, 125 A.D.3d 531, 532 (1st Dep't 2015) (applying "life or safety" FOIL exemption to avoid disseminating a "trove" of information which could be "potentially exploited by terrorists"); *Matter of Goyer v. N.Y. State Dep't of Envtl. Conserv.*, 12 Misc. 3d 261, 272 (Sup. Ct. Albany Cty. 2005) (the "life or safety" exemption applied to sustain an agency's decision to exempt from FOIL disclosure data about the home locations of individuals who owned recreational firearms).[8]

A recent judicial decision upholding a decision of the Metropolitan Transportation Authority ("MTA") not to disclose sensitive infrastructure-related information based on the "life or safety" FOIL exemption is instructive. In *Matter of Rankin v. Metropolitan Transportation Authority*, the court considered whether to require the MTA to disclose records describing the New York City subway system and stations in detail. 2010 WL 3285633 (Sup. Ct. N.Y. Cty. Aug. 10, 2010). The MTA submitted affidavits describing how disclosure of the requested information "would enable a potential terrorist to plan a more effective surreptitious attack" on the subway system. *Id.* at *9. The affidavits also described recent interrupted plots to disrupt the subway system in order to support the MTA's claim that the subway is a terrorist target and that the safety concerns were more than speculative. *Id.* This information satisfied the agency's burden of demonstrating that the records sought fell squarely within the "life or safety" FOIL exemption and were therefore not required to be disclosed. *Id.* at *12.

[8] "When analyzing and deciding issues pertaining to Freedom of Information Law (FOIL) exemptions patterned after the federal Freedom of Information Act (FOIA), New York courts may look to federal case law for guidance." *Matter of Abdur-Rashid v. N.Y. City Police Dep't*, 45 Misc. 3d 888, 890 (Sup. Ct. N.Y. Cty. 2014); *see also Matter of Fink v. Lefkowitz*, 47 N.Y.2d 567, 572 (1979) ("Federal case law and legislative history on the scope of [FOIL] exemption[s] are instructive.").

Likewise, in this case, there is sufficient evidence demonstrating that the Conduit Location Information falls squarely within the "life or safety" FOIL exemption. As explained above, disclosure of the redacted information would reveal the sensitive details about the communications network, and could enable a terrorist or other bad actor to identify crucial locations in the conduit system where damage to could a large scale disruption of communication services. *See, e.g.*, Dempsey Aff. ¶¶ 8-9. Alternately, the information could be used to identify remote areas where damage to cables would result in service interruptions at high profile targets including law enforcement and government buildings, banks, financial and data centers and cable landing stations. *Id.* In addition, the incidents in California and Arizona show that fiber networks like the conduit system are currently and will continue to be targets for specific attacks.

Moreover, federal and state agencies have acknowledged the critical role that communications infrastructure plays in emergency situations. The United States Department of Homeland Security considers these services to be part of the country's "Communications Sector." *See Critical Infrastructure Sectors,* United States Department Of Homeland Security, http://www.dhs.gov/critical-infrastructure-sectors (last visited January 17, 2017). They are considered "critical infrastructure" because the incapacitation or destruction of TWC's and other similar systems and networks "would have a debilitating effect on security, national economic security, [and/or] national public health or safety." *Id.* Likewise, the Chair of the New York State Public Service Commission has written that "telecommunications services and networks . . . are a backbone to New York State's public health, safety and general welfare, including the state's ability to recover from natural disasters. . . ."[9]

[9] *See* Letter from Audrey Zibelman to the New York State Assembly (May 13, 2014) http://www.cwa1108.org/1108_Zibelman%20Letter%20to%20Leg%20Leaders%205-13-14.pdf (Bucki Aff. Ex. E).

The *Rankin* decision specifically stated that disclosure of information such as the "location of electrical, computer and other equipment" could have a "potentially devastating effect" if handed over to terrorists who wanted to maximize damage to the subway system. 2010 WL 3285633 at *13. While the *Rankin* court was describing the effect of revealing the location of subway routes and technology, the same reasoning applies to disclosing the location of the City's information routes and technology housed in the ECS conduits.

III. The Requested Information Is Exempt From Disclosure Under Section 87(2)(d)'s "Trade Secret" Exemption.

FOIL also permits an agency to deny access to records that "are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise." N.Y. PUB. OFF. LAW § 87(2)(d). This statutory provision actually "create[s] two separate FOIL exemptions," "one that exempts all records proven to be bona fide trade secrets, and another that requires a showing of substantial competitive injury in order to exempt from FOIL discovery all other types of confidential commercial information imparted to an agency." *Matter of Verizon N.Y. Inc. v. N.Y. State Pub. Serv. Comm'n*, 137 A.D.3d 66, 69-70, 23 N.Y.S.3d 446 (3d Dep't 2016). The information at issue here is protected under both of these exemptions.

A. The Intervenors' Information Constitutes Trade Secrets.

To determine whether particular information constitutes a trade secret, the Court first must determine whether it is a "'formula, pattern, device or compilation of information which is used in one's business, and which gives [one] an opportunity to obtain an advantage over competitors who do not know or use it.'" *Matter of N.Y. Tel. Co. v. Pub. Serv. Comm'n*, 56 N.Y.2d 213, 219 n.3 (1982) (quoting RESTATEMENT OF TORTS § 757, cmt. b). "Second, if the

information fits this general definition, then an additional factual determination must be made 'concerning whether the alleged trade secret is truly secret . . . .' *Verizon N.Y.*, 137 A.D.3d at 72 (quoting *Marietta Corp. v. Fairhurst*, 301 A.D.2d 734, 738 (2003)). The Court considers a number of factors in connection with this latter determination, including "(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; [and] (6) the ease or difficulty with which the information could be properly acquired or duplicated by others." *Marietta Corp.*, 301 A.D.2d at 738 (internal quotations marks, brackets, and citations omitted).

This test is easily satisfied here. Information regarding the location and extent of each carrier's conduit runs constitutes a "compilation of information" used in their businesses, and one that gives them an advantage over competitors who do not have the information. Intervenors expended considerable sums in planning and deploying their network, and did so in order to attempt to gain an advantage over competitors. *See, e.g.*, Dempsey Aff. ¶ 10; Affidavit of Charmaine Stradford, sworn to on Jan. 23, 2017 ("Stradford Aff.") ¶¶ 5, 18.

AT&T, for example, competes for customers in the City by constructing sophisticated and customized networks, and making important strategic budgeting and other business decisions with respect to deploying construction, maintenance and marketing resources and identifying where its network facilities are best positioned in order to serve commercial customers in New York City. Stradford Aff. ¶¶ 5, 14 AT&T has invested significant time and financial resources into developing and building out its networks, and marketing them to consumers. *Id.* ¶ 18.

Moreover, AT&T uses its closely-held information regarding its network capabilities and the extent of its network at various locations to attempt to obtain advantages over its competitors, including in marketing its networks and in investing to build out its network at locations that AT&T finds strategic. *See id.* ¶¶ 5, 14. If AT&T's competitors could obtain this information, because it was publicly available, they could use it to garner significant insight into AT&T's strategic network builds, and easily learn where AT&T has significantly built out its network, and where it has not. *Id.* ¶ 12. AT&T's competitors could then adjust their own plans accordingly, and alter their own network and resource allocations to replicate AT&T's network and/or exploit those areas where AT&T has not built out its network. *Id.* Competitors could also use the information at issue to exploit "network design gaps" and make sales pitches to customers in locations where the competitor's network has a superior infrastructure, follows a more direct route, or encompasses more diverse routes than AT&T's network. *Id.* All the same is true of the other Intervenors' network information. *See, e.g.*, Dempsey Aff. ¶¶ 11-12.

In addition, this compilation of information is "truly secret" (*Marietta Corp.*, 301 A.D.2d at 738), and not already publicly available as Petitioner wrongly suggests. *See* Pet'r's Mem. at 13, 19. Pursuant to *Marietta Corp.*, the first three pertinent factors are "(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; [and] (3) the extent of measures taken by the business to guard the secrecy of the information." 301 A.D.2d at 738. All of the Intervenors take strict measures to guard the secrecy of the detailed network information at issue here, even within their companies, and this information is not widely known outside of the business (apart from, *e.g.*, ECS, DoITT, and others with a "need to know").

The Intervenors routinely treat as confidential and proprietary information regarding the specific location of their facilities, including, in particular, information showing the specific location of fiber optic and copper cable runs and the access points for such routes, such as specific manholes. *See* Stradford Aff. ¶ 9; Dempsey Aff. ¶ 14.

Further, the Intervenors have established practices and procedures to protect the confidentiality of information about their specific network routes. For example, AT&T has an established written policy and process governing requests for proprietary network information, including records or maps showing the physical locations of its network facilities. Under that policy, street-level map information is provided to a customer only in certain narrow circumstances, following a detailed process for review and approval of the request for such information. This information is shared only if, among other things, the customer has executed a non-disclosure agreement; the information is limited to the facilities serving the customer, and does not include other routes; and absent additional approvals and a demonstrated need, the map information remains in AT&T's possession and control and the customer is not permitted to copy the information. Moreover, even when specific map information is provided to a customer, the map excludes any cable or count information (such as the number of conduits or ducts); supporting structure and network details, including manhole numbers; and any scaling below street-level detail, such as any identification of the side of the street where the facilities are situated. Stradford Aff. ¶ 9.

Similarly, to maintain the physical security of its network, TWC supervises all underground excavation conducted by ECS. Dempsey Aff. ¶ 13. These initiatives cost TWC approximately $3.6 million per year. *Id.* To maintain the confidentiality of its network, TWC only provides information about its network's locations and structure to outside entities if they

sign a strict non-disclosure agreement. *Id.* ¶ 14. When TWC does provide outside entities with information, it is sanitized to remove sensitive details. *Id.*

Access to detailed network information is restricted even within each Intervenor's business. TWC, for example, maintains conduit and infrastructure information in a database that is not accessible unless the TWC employee is properly credentialed. Dempsey Aff. ¶ 14. If an employee leaves the company, his or her credentials are shut off. *Id.* *See also* McDermott Aff. ¶ 4 (explaining AT&T's similar policies).

Petitioner asserts that the conduit paths are already public knowledge because customers of ECS make conduit occupancy information available to the public. Pet'r's Mem. at 15, 20. But Petitioner has identified only a handful of ECS customers who make maps of their facility routes publicly available. Moreover, these maps do not have the same level of detail as the data at issue in this case, and do not identify specific manhole locations where those facilities could be accessed. Furthermore, while a few providers may provide maps of their conduit routes, Intervenors do not. McDermott Aff. ¶ 2; Stradford Aff. ¶ 9; Dempsey Aff. ¶¶ 8, 13. Thus, even if a person could determine the location of another ECS customer's facilities in the City, this would provide no information about what manholes a person could use to access the facilities of Intervenors (or, for that matter, the NYPD, the Unified Courts, or the Federal Reserve, all ECS tenants who do not make such maps publicly available).

The fourth and fifth factors in determining whether the information is "truly secret" are "(4) the value of the information to the business and its competitors; [and] (5) the amount of effort or money expended by the business in developing the information." *Marietta Corp.*, 301 A.D.2d at 738. As explained above, the information at issue has significant value to the Intervenors and to their competitors. Each Intervenor has invested considerable resources in

building out its network, and in making strategic choices about where, when, and how to place network facilities in order to compete. If competitors could obtain the detailed network information of another carrier, they could use that information to identify both locations where the carrier has expended considerable resources to build infrastructure to compete, and locations where the carrier has gaps in its network. *See* Stradford Aff. ¶¶ 11-18; Dempsey Aff. ¶¶ 11-12. As noted above, each of the Intervenors also incurs significant effort and expense to maintain the confidentiality of its network information, including instituting policies and procedures to limit access to that information.

The sixth and final factor in determining whether information is "truly secret" is "(6) the ease or difficulty with which the information could be properly acquired or duplicated by others." *Marietta Corp.*, 301 A.D.2d at 738. It would be extremely difficult, if not impossible, for others to duplicate the detailed network information at issue here. Petitioner notes that manhole locations are publicly observable by visual inspection. Pet'r's Mem. at 13-14. But such visual inspection tells one little or nothing about what is in the manhole, including what facilities, the number of facilities, the number of users relying upon conduit in that location, and the identity of those users. Nor does it tell one anything about other manholes to which conduit in that particular manhole may run. *See* Stradford Aff. ¶¶ 7-8.

Petitioner also notes that ECS tenants are allowed access to the underground conduit for the purpose of maintaining their own cables, and suggests that an ECS tenant could ascertain by physical inspection which of its competitors have cables at a given location. Pet'r's Mem. at 20. But while a competitor could potentially determine whether others run conduit at *one* manhole location to which the competitor has access, a competitor would have to invest significant time, expense and effort to map the presence of other providers at *all* manholes across the City,

including the 10,530 manholes under ECS' control across the 90 square miles of the Bronx and Manhattan. The data requested by Petitioner would allow a competitor to obtain that valuable information at little or no cost. *See* Stradford Aff. ¶ 8.

In short, the information sought by Petitioner constitutes trade secrets. As a result, that information is exempt from disclosure under N.Y. PUB. OFF. LAW § 87(2)(d).

B. Intervenors' Network Information Is Derived From Information Obtained From Commercial Enterprises Which If Disclosed Would Cause Substantial Injury To Their Competitive Position.

The records at issue also are exempt from disclosure because they are records "submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise." N.Y. PUB. OFF. L. § 87(2)(d).

As a threshold matter, while the spreadsheet at issue was submitted to DoITT by ECS, that does not mean (as Petitioner has wrongly contended, Pet'r's Mem. at 18-19) that the statute protects only the competitive position of ECS itself. The statute expressly protects not just information submitted directly to an agency by a commercial enterprise, but also information "derived from information obtained from a commercial enterprise," the disclosure of which would cause competitive harm to the enterprise. N.Y. PUB. OFF. L. § 87(2)(d). The information at issue regarding Intervenors' facilities is derived from information obtained from Intervenors, because it reflects their strategic choices about where to deploy its facilities and which (and how many) conduits to lease from ECS. As such, this information is fully within the scope of Section 87(2)(d).

Moreover, release of the information would cause substantial injury to the competitive positions of Intervenors. The test for whether FOIL disclosure of commercial information would cause substantial injury to a company's competitive position is derived from the holding in

Matter of Encore College Bookstores, Inc. v. Auxiliary Service Corp. of the State University of New York at Farmingdale, 87 N.Y.2d 410 (1995). Whether substantial competitive harm exists:

> turns on the commercial value of the requested information to competitors and the cost of acquiring it through other means. Because the submitting business can suffer competitive harm only if the desired material has commercial value to its competitors, courts must consider how valuable the information will be to the competing business, as well as the resultant damage to the submitting enterprise. Where FOIA disclosure is the sole means by which competitors can obtain the requested information, the inquiry ends here.

Id. The court in *Encore Books* further explained that:

> [b]ecause competition in business turns on the relative costs and opportunities faced by members of the same industry, there is a potential windfall for competitors to whom valuable information is released under FOIA. If those competitors are charged only minimal FOIA retrieval costs for the information, rather than the considerable costs of private reproduction, they may be getting quite a bargain. Such bargains could easily have competitive consequences not contemplated as part of FOIA's principal aim of promoting openness in government.

Id. In order to establish applicability of the "competitive harm" FOIL exemption, a company is not required to demonstrate actual harm, but rather actual competition and a likelihood of substantial competitive injury. *Encore Books*, 87 N.Y.2d at 421; *see also Matter of Aurelius Capital Management, LP v. Dinallo*, 2009 WL 367770, at *2 (Sup. Ct. N.Y. Cty. Jan. 13, 2009).

This standard has been applied to protect many different commercial interests. In *Encore Books*, a bookstore at a state university was not required to give its competitor a booklist compiled for the school store by Barnes & Noble. *Encore Books*, 87 N.Y.2d at 420. Because the list was accumulated "by virtue of the effort and expense of Barnes & Noble," the court reasoned that compelling disclosure would enable the competitor bookstore to obtain information "without expending its resources, thereby reducing its cost of business and placing Barnes & Noble at a

competitive disadvantage." *Id.* at 421. As a result, the information fell squarely within the FOIL exemption for information which would cause competitive harm if disclosed. *Id.*

Applying the rule from *Encore*, the court in *Aurelius Capital Management* upheld the State of New York Insurance Department's refusal to turn over data collected by the Department from a private insurance company. 2009 WL 367770 at *1. The court explained that the private insurance company's information had commercial value to the petitioner, was not readily available elsewhere, and would cost much more to assemble than the cost of seeking the data through FOIL. *Id.* at *3. Based on these facts, the court found that disclosure of the information would have caused the insurance company to suffer a substantial injury to its competitive position in the market. *Id.* at *4. Therefore disclosure was not required. Likewise in *Matter of Verizon New York, Inc. v. Mills*, 60 A.D.3d 958 (2d Dep't 2009), the court refused to order the disclosure of franchise reports by Verizon which "contained a trove of information compiled by Verizon that would allow [its competitor] Cablevision to target Verizon's actual and potential customers with respect to various services." *Id.* at 960.

Based on the *Encore Books* holding, another court explained that "documents should be exempt from disclosure where disclosure would give an unfair advantage to competitors because they would be in a position to learn customized information" about their competitors and then use this information to tailor their efforts to better compete. *Matter of James, Hoyer, Newcomer, Smiljanich & Yanchunis, P.A. v. State, Office of Att'y Gen.*, 2010 WL 1949120, at *9 (Sup. Ct. N.Y. Cty. March 31, 2010).

As in these cases, each Intervenor's detailed network information has commercial value to the competitors of the Intervenor. As explained above, disclosure of the information would enable the Intervenor's competitors to identify the locations where it has expended considerable

resources to build infrastructure to service customers. *See, e.g.*, Dempsey Aff. ¶ 11. It also would allow the Intervenor's competition to determine where the Network Intervenor has not yet tapped a significant percentage of the market and allow the competition to beat it to that location. *Id.* ¶ 12.

Similarly, AT&T develops customized network solutions ("UVN rings") for its high-value enterprise customers based on the customers' individualized needs. The data requested by Petitioner would enable members of the public, including AT&T's competitors, to guess the identity of AT&T's UVN customers based on the customers' proximity to manholes or conduits where the data shows that AT&T had concentrated its facilities. From a visual inspection of the physical manhole and conduit, a person would then be able to determine the size of the conduits within a manhole, the size and number of strands within the conduits, the types of cable used, whether the cable is copper or fiber, AT&T's investment for that particular customer, the bandwidth capability of AT&T's facility, and the characteristics of data transmitted by such conduits. AT&T's competitive position would be harmed, not only because a competitor could exploit such information in soliciting UVN customers, but also because UVN customers value security and confidentiality, so that public access to such information would undercut a critical element of AT&T's business product offering. *See* Stradford Aff. ¶¶ 14-16.

Finally, as demonstrated above, this kind of detailed information about the Intervenors' networks is currently unavailable from any other source. *See* Dempsey Aff. ¶ 8; Stradford Aff. ¶¶ 6-8. In accordance with *Encore Books*, the inquiry should stop there, and disclosure should be denied pursuant to Public Officers Law § 87(2)(i). However, Intervenors further note that, as explained above, it would be extremely difficult or impossible for others to duplicate the detailed network information at issue here. As a result, if that network information were disclosed,

competitors of each Intervenor would receive a windfall of economically valuable data on which to build a market strategy. Because disclosure of the detailed network information at issue would confer a competitive advantage on competitors, it falls squarely within the "competitive harm" exemption from FOIL disclosure.

Conclusion

For the foregoing reasons, Intervenors respectfully request that the Court deny the Article 78 Petition.

Dated: February 3, 2017

Thomas M. Smith, Esq.
Eckert Seamans Cherin & Mellott, LLC
10 Bank Street, Suite 700
White Plains, NY 10606
Attorneys for Intervenor-Respondent RCN Telecom Services, LLC

By: /s/ Thomas M. Smith CRB
THOMAS M. SMITH

Douglass B. Maynard, Esq.
Jessica Oliff Daly, Esq.
Akin Gump Strauss Hauer & Feld LLP
One Bryant Park
New York, NY 10036
Attorneys for Intervenor-Respondent Time Warner Cable Inc.

By: /s/ Douglass B. Maynard CRB
DOUGLASS B. MAYNARD

Craig R. Bucki, Esq.
Phillips Lytle LLP
The New York Times Building
620 Eighth Avenue, 23rd Floor
New York, New York 10018

Hans J. Germann
Mayer Brown LLP
71 S. Wacker Drive
Chicago, IL 60606
Attorneys for Intervenor-Respondent AT&T Corp.

By: Craig R. Bucki
CRAIG R. BUCKI