SUPREME COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY

PRESENT: HON. JOAN B. LOBIS PART 6
*Justice*

SUSAN CRAWFORD,

Petitioner,

- v -

NEW YORK CITY DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS, et. al.,

Respondents.

INDEX NO. 157002/2015

MOTION DATE 4/4/2017

MOTION SEQ. 001

The following papers were read on this Article 78 petition.

| | PAPERS NUMBERED |
|---|---|
| Notice of Petition/ Order to Show Cause – Affidavits – Exhibits | 1-5,66-68, 74-77, 81-83, |
| Answering Affidavits – Exhibits | 18, 21-39, 45-47, 58, 130-31, 133, 137-150 |
| Replying Affidavits | 161-163 |

**MOTION DECIDED IN ACCORDANCE WITH ACCOMPANYING DECISION AND ORDER**

Dated: May 11, 2017

JOAN B. LOBIS, *J.S.C.*

1. CHECK ONE: ..... X CASE DISPOSED ☐ NON-FINAL DISPOSITION
2. CHECK AS APPROPRIATE:....PETITION IS ☐ GRANTED ☐ DENIED X GRANTED IN PART ☐ OTHER
3. CHECK IF APPROPRIATE: ..... ☐ SETTLE ORDER ☐ SUBMIT ORDER ☐ DO NOT POST
☐ FIDUCIARY APPOINTMENT ☐ REFERENCE

**SUPREME COURT OF THE STATE OF NEW YORK**
**NEW YORK COUNTY: IAS PART 6**

----------X

In re Application for a Judgment under Article 78 of the Civil Practice Law and Rules by
SUSAN CRAWFORD,

Petitioner,

Index No. 157002/2015

-against-

**Decision & Order**

NEW YORK CITY DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS, AT&T CORP., EMPIRE CITY SUBWAY COMPANY LTD., TIME WARNER CABLE INC., and RCN TELECOM SERVICES, LLC,

Respondents.

----------X

In this proceeding Professor Susan Crawford asserts that respondent New York City Department of Information Technology and Telecommunications (DOITT) improperly withheld information she sought in her Freedom of Information Law (FOIL) request. She seeks an order directing DOITT to provide her with immediate access to all requested information that is not exempt, along with attorneys' fees. Public Officers Law §89(4)(c). This Court has granted the motions to intervene of AT&T Corporation (AT&T), Empire City Subway Company Ltd. (ECS), Time Warner Cable Incorporated (Time Warner), and RCN Telecom Services, LLC (RCN), and denied DOITT's pre-answer cross-motion to dismiss.

The telecommunications conduit system contains ducts which carry copper, coaxial, and fiber-optic telecommunications cables from manhole to manhole. The manholes provide access to the conduits. Not only do the cables transmit telephone, television, and internet services to individuals and businesses, but they provide these services to the police and fire

departments, the state and federal court systems, hospitals, and banks including the federal reserve. DOITT is charged with protecting the city's information technology (IT) infrastructure and systems, ensuring vendor accountability, providing all New Yorkers with access to IT, and obtaining broadband access to residents of underserved communities. DOITT manages the infrastructure, and ECS, which owns and manages all underground conduits in Manhattan and the Bronx, builds and maintains the conduits and leases them to internet providers including the commercial respondents in this proceeding.[1] As part of DOITT's mandate to provide IT services throughout the city, it must ensure that ECS "effectively and efficiently mak[es] conduit available to Internet service providers as needed by them and in a manner that promotes affordable Internet access to New York residents." Crawford Aff., ¶ 14.

Petitioner Professor Susan Crawford, a Harvard Law School professor and a director of Harvard's Berman Klein Center for Internet & Society, has advocated extensively for net neutrality.[2] She argues that internet access should not be controlled by corporate providers because this does not foster net neutrality and results in overly high prices for internet access. She states that providers offer high-speed internet to high-income neighborhoods, and that low-income areas have limited or no internet access. This, she says, increases the disadvantages low-income families face. Further, she contends, because of their relative monopolies on control of the conduit,

[1] ECS has a monopoly over the conduit and manholes relating to telecommunications services pursuant to an 1891 contract. Petitioner notes that there have been no revisions to the contract. The conduit is made of either iron pipe, vitrified clay, creosoted wood, plastic, fiberglass, or concrete. ECS states that the vast majority of the new conduit it constructs use plastic ducts.

[2] With net neutrality, all information can travel throughout the internet freely, without regard to the content and without roadblocks making it less accessible to the public. Without it, a provider can prioritize information, sending its own content over the internet at faster speeds than other content or even blocking certain content and distributors of information.

providers have no incentive to replace outdated wires with faster, more efficient fiber optic ones. She has published studies on the availability of high speed internet access in cities including Washington, D.C.; Seattle, Washington; Leverett, Massachusetts; and San Francisco, California.

Currently, Professor Crawford is researching "whether the City of New York is fulfilling its mandate of making high speed Internet access reliable and competitive to meet the needs of New Yorkers" regardless of their income level. Crawford v. New York City Dep't of Information Techn. and Telecommunications, 43 Misc. 3d 735, 738 (Sup. Ct. N.Y. County 2014)(Crawford I), lv dismissed, 136 A.D.3d 591 (1st Dep't 2016). She alleges that "[m]ore than a quarter of New York City households do not have access to high-speed internet today," Mem. of Law in Support of Petition, p.1, and that the greatest disparity occurs among "minorities and low-income residents." Id. Her research will, among other things, focus on whether low-income and minority neighborhoods lack the infrastructure necessary to provide them with affordable high speed cable service, and why New York City's cable service is half the speed of and four times as expensive as that of other states in the United States and major cities throughout the world. She states that the only way to evaluate the inequities in the system is with information about the endpoints and occupancy of existing conduit.

On January 24, 2012, Professor Crawford and her then-research assistant Anjali Dalal served a Freedom of Information Law (FOIL) request on DOITT. Among other things, they sought "1. The geographic location of conduit owned by Empire City Subway ("ECS"). 2. The geographic location of conduit operated by ECS." Id. DOITT denied the 2012 FOIL request as to these items under Public Officers Law (POL) § 87(2)(i), which states that agencies need not make

records available in response to a FOIL request if the disclosure would "would jeopardize the capacity of an agency or 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 . . . ." Professor Crawford and Ms. Dalal appealed. DOITT denied the appeal on August 2, 2012, both on the original basis, POL § 87(2)(i), and on the ground that the material, if disclosed, "could endanger the life or safety of any person." POL § 87(2)(f).

Professor Crawford and Ms. Dalal commenced an Article 78 proceeding challenging this determination. Crawford I, 43 Misc. 3d 735. Justice Shlomo Hagler, who presided over Crawford I, evaluated the applicability of the information technology (IT) exemption. POL § 87(2)(i). DOITT stated that information about the locations of ECS-owned or -operated conduit were available only in the form of forty-one detailed maps, the release of which could jeopardize the security of its IT assets. The Court inspected, in camera, a representative sample of the documents and expert testimony. It held the maps were exempt because of the impossibility of redacting exempt information from them but directed respondent to conduct a diligent search "to discover other responsive documents . . . which provide petitioners with non-sensitive and non-exempt general information" responsive to their request. Id. at 744.

On May 9, 2014, Professor Crawford submitted a new FOIL demand in which she asked for documents other than maps that provided the information she sought. On January 30, 2015, in response to Professor Crawford's request for a list of ECS-owned conduit broken down by block, zip code, neighborhood, and other discrete regions, DOITT provided a spreadsheet inventory it recently had obtained, in which "information identifying the location of the manholes

(the endpoints of each conduit), the number of tenants utilizing each conduit, and the names of tenants leasing conduit space" was redacted. Petitioner's Mem. in Support, p.8.[3]

In her February 26, 2015 appeal, Professor Crawford contended that the spreadsheet did not explain its headings or content and that the redactions made it impossible to understand the significance of the unredacted information or obtain the data she needed. The disclosure was not excludable under the IT exemption, POL § 87(2)(i), she said, because the information would not enable access into a database, provide a password, or otherwise enable remote access to the cables and thus would not impact the underlying technology. Further, she stated, even if "physical technology assets" could be excluded under POL § 87(2)(i), the exemption was not applicable here because the excluded information – "the number of conduits running from one specified location to another specified information, how many of those conduits are in use, and the name of the customer utilizing those conduits" – does not show the route of the conduit from one location to the next. Crawford Appeal Letter, Feb. 26, 2015, p.2. In addition, Professor Crawford asserted that the redaction in the spreadsheet of location information for all of the conduits – over 200,000 in Manhattan alone – was overly broad. She suggested that, for example, DOITT could disclose "the conduit available in locations that are not currently served by any high-speed broad band access" as this "could be disclosed without any significant security or safety concerns being presented." Id. She argued disclosure would serve the public's significant interest in "understanding the communications infrastructure and its capabilities in New York City," id., and might facilitate

[3] All that remains in the spreadsheet are "from MH#," "to MH#" – with the locations of these manholes redacted – and the "Duct#."

market growth and increase open fiber installations. Professor Crawford also sought the customer list, which DOITT had redacted.

In its March 15, 2015 decision, DOITT granted Professor Crawford's request to the limited extent of providing a list of ECS's conduit tenants which did not include the conduits' locations or the number of conduits the tenants occupied. In omitting this information, DOITT relied on the trade secret exemption in POL § 87(2)(i). The decision additionally denied her request for an unredacted copy of the spreadsheet in full. DOITT stated that disclosure of the location of the ECS-owned or -controlled manholes would create or increase a security risk. It concluded that the redacted information on the spreadsheet was as sensitive as the information on the maps, reasoning that because of their proximity to each other, disclosure of the manholes' locations would necessarily disclose the conduit's approximate location. It claimed that her suggestion that DOITT provide information concerning communities without high-speed access was improper because DOITT was not obligated to interpret petitioner's original request. Further, it stated, because the city's contracts with cable franchisees require them "to make cable television service available to all New York residents, we might infer that those franchisees have made high-speed broadband available to all New York residents as well." DOITT Appeal Determination, March 12, 2015, p.2. Because unused conduit space may be used someday, DOITT stated, the request for disclosure of those locations would endanger the security of both hypothetical future tenants and tenants currently at the locations.

After the March 2015 determination, Professor Crawford filed the current Article 78 proceeding. She emphasizes that unlike most Article 78 challenges, in those concerning FOIL

requests the court must presume the records are disclosable. Therefore, the court does not review the decision with deference, and the burden is on the respondent to justify the nondisclosure. DOITT does not show that the IT exemption applies, she argues, because under the prevailing case and statutory law it only is applicable where a real and substantial threat exists. Here, she contends, DOITT has not shown a substantial likelihood that disclosure of the redacted information on the spreadsheet would endanger the entire IT structure or increase the existing threat to government buildings, banks, data centers, and the cable system. Instead, Professor Crawford argues, DOITT does little more than repeat the applicable statutory language and add that Crawford I applies.

Further, she states, Crawford I involved maps which included a detailed depiction of the city's fiber optic network as well as routing information and the points of entry for high-profile targets. The unredacted spreadsheets at issue here do not create this risk, Professor Crawford states, because they do not show the specific paths of the conduits, just the manholes through which they flow. Other information that has been removed, and which she contends is not excludable, includes "the number of conduits, conduit capacity and availability of unused conduits on a manhole by manhole basis." Crawford Mem. in Support, pp. 9-10. Moreover, she argues, ECS manholes are identifiable by their covers, and interested individuals can determine where they are located even in high-risk areas. In addition, she says, internet service providers (ISPs) "often publish maps of their own networks revealing cable paths in substantial detail" and share conduit locations online. Id., p.10. Thus, disclosure will not significantly enhance the existing risk.

Even if some redaction is appropriate, petitioner argues, DOITT has been overly broad in its interpretation of the exclusion. She contends that DOITT has withheld all information

in the spreadsheet based on its argument that some of it might be excludable, rather than – in compliance with its duties under FOIL – withholding only information revealing the direct paths to high-profile, high-risk areas. She notes that the agency "refused even to provide conduit information for underserved and low-risk residential neighborhoods with no high risk terrorist targets . . .," id., p.16, and states "such information would still help [petitioner] to identify areas that lack access to high-speed internet because of inadequate conduit infrastructure, and to define underserved areas where new competitors could enter relatively quickly because vacant conduit is available." Id., p.17. As DOITT can redact any allegedly sensitive information without undue effort, she states, the rest of the spreadsheet must be disclosed. She argues that information about the conduits "on a neighborhood-by-neighborhood basis would not raise the same concerns" upon which DOITT and Crawford I relied because DOITT can exclude conduits located near high-profile targets. Id. Moreover, petitioner contends, DOITT is wrong in stating that because Professor Crawford requested information about all of the conduit, it had no obligation to comply with her subsequent suggestion that it redact only the locations of high-profile targets and neighborhoods. This position "gets it exactly backwards," she states, because DOITT rather than petitioner is to narrow the scope of the disclosure in a way that provides the most information while protecting government security and other interests. Id., p.16.

Petitioner further argues that the spreadsheet is not excludable under the trade secret exemption, which applies when the information causes "substantial injury to the competitive position of the subject enterprise." POL § 87(2)(d). She states that DOITT's premise – that it is the only source of the location of the conduits that the additional respondents occupy – is incorrect. Instead, ECS has this information and grants tenants of the conduits access so they can install and

maintain their cables, and that they are able to identify the other tenants when they do so. Moreover, she notes, some ECS customers have made their conduit locations publicly available, and the federal and state governments have released broadband maps showing which ISPs provide coverage in various neighborhoods and pointing out which of the ISPs in these areas provide high-speed service. She states that the spreadsheet is not a trade secret because it was DOITT which created it using information from the commercial respondents.[4]

Petitioner points out that there is a strong public interest in making this information available, which also is critical to her efforts to analyze the disparity of high-speed internet access in the city and to assess DOITT's performance in carrying out its mandate to provide such access citywide. She states the information may reveal that a lack of competition or an insufficient amount of conduit has caused or exacerbated the current inequities. She states that according to a 2010 report by the New York City Comptroller, many conduits are vacant, and Verizon – which owns ECS – occupies a large percentage of the more newly constructed conduits. She concludes that the failure of DOITT and ECS to fulfill their mandates harms not only her but the public at large.

DOITT has filed its answer and redacted copies of its supporting papers.[5] In addition to denying all allegations of wrongdoing, it stresses the importance of the city's

[4] Petitioner further notes that in some neighborhoods DOITT permits microtrenching, which allows telecommunications services to install fiber-optic cable more rapidly and at lower cost in the joints between the sidewalks and the curbs or the streets with the understanding that "[t]he map[s of their routes] may be made public . . . in the discretion of [DOITT]." DOITT Microtrenching Rule § 1-0(e)(b (June 24, 2013). This is not directly at issue here, although according to petitioner it shows the increased availability of information about the location of fiber optic cable.

[5] As the parties stipulated, DOITT provided the parties and the Court with unredacted copies of its responsive papers, which provide more detail on how the unredacted spreadsheet could be used.

infrastructure of conduits and manholes, through which wires run that provide phone, cable, and internet services to residents, businesses, and government agencies such as the police and fire departments, the Federal Reserve Bank, and the state and federal courts. DOITT states that there are around 58 million feet of electrical conduits, connected within approximately 11,000 manholes, and that ECS, which controls and maintains them all, leases the space within the conduits to numerous parties including the additional respondents. It states that the banking and other financial transactions which are carried through the conduits constitute "highly sensitive commercial information." Ans., ¶ 35. It adds that the cables are "vulnerable" to "cutting, melting, and other acts of vandalism" because of their proximity to the city's streets. Id., ¶ 36. It claims that the disclosure of this locational information would raise security issues, and that disclosure of the locations of the manhole covers under which conduit runs would reveal the location of the conduits within a few feet. With this knowledge, it states, individuals can track the paths of the conduits within a few feet as well.

Citing the affidavit of Chief James Waters, the head of NYPD's Counterterrorism Bureau, DOITT states that "the unredacted spreadsheet could easily be used to construct a map of the City's conduit infrastructure and corresponding fiber optic networks," Id., ¶ 59, and thus the networks would be vulnerable to cyberattacks and physical attacks. In particular, Chief Waters states in his affidavit, the attacks could result in system-wide disruptions, economic loss due to the disruption of the stock exchange, banks and other financial institutions, and loss of human lives because of potential disruptions to the police and fire departments' communication systems and to hospitals' abilities to access their records. Moreover, he states, it will be expensive and time-consuming to repair the damage to the cables. He points out that fiber optic cables were cut on

several occasions in the San Francisco Bay area, causing disruption, and therefore the threat is not hypothetical. He annexes a list of terrorist attacks that were contemplated or planned in New York City, including numerous attempts to set off bombs and a plan to attack subway passengers by dispersing canisters of hydrogen cyanide. He additionally annexes an affidavit submitted in Crawford I which discusses potential dangers related to the disclosure of the maps. The implication is that because the material petitioner seeks allegedly would enable interested parties to reconstruct the maps, the dangers here remain the same. Based on the above, DOITT states, it has established that disclosure of the records would jeopardize its ability to guarantee the security of its electronic information systems and its IT infrastructure. Therefore, the material is exempt from disclosure.

Like DOITT, ECS contends in its answer that DOITT properly withheld the information in question. It argues the applicability of POL 87(2)(i), because DOITT would no longer be able to guarantee the safety of the IT assets, and POL § 87(2)(f), in that disclosure could endanger human life or safety.[6] In its supporting memorandum, ECS states that although it provides information about its operations to DOITT, its supervisor, it does so subject to confidentiality and clearly marks certain documents as confidential. ECS states that this is the case with the spreadsheet Professor Crawford currently seeks.

In arguing that the redacted information should remain confidential, ECS relies in part on FOIL's IT exemption on the ground that disclosure would jeopardize its capacity to "guarantee the security of its information technology assets," including infrastructures. POL §

[6] In addition, it states the information is exempt under POL § 87(2)(d) because of the harm to the commercial respondents' competitive position. The commercial respondents address this issue.

87(2)(i). Citing TJS of N.Y., Inc. v. N.Y. State Dep't of Taxation and Finance, 89 A.D.3d 239, 243 (3rd Dep't 2011)(TJS), it states that this exemption protects the "assets themselves" from electronic attack. It argues that Crawford I applied the IT exemption to the conduit routes, finding that "[m]ore numerous attacks on 'high value cables' . . . could be 'catastrophic,'" Crawford I, 43 Misc. 3d at 742, and that the possibility of attacks has, if anything, increased since that time. It cites to the affidavits of Robert F. Connolly, ECS vice-president, who contends the information is sensitive and proprietary; and of Michael A. Mason, chief security officer at Verizon, who states that if DOITT provided the unredacted spreadsheet to Professor Crawford it "would create a security risk to the City and its critical communications infrastructure." Mason Aff., ¶ 14.

Additionally, ECS states that FOIL's public safety exemption, POL § 87(2)(f), is applicable. ECS stresses that it is not required to show that a particular person will be in danger if the information is disclosed. Moreover, ECS contends, it need not describe the risks in detail because this would expose the very information it aims to protect. Mr. Mason, the Verizon security officer, contends that although the manhole locations are publicly discernible the conduit routes are not, and this is for security reasons. ECS states that disclosure would increase the risk of bombing the underground communications network – and, in addition, would threaten the lives of individuals who might be working in the manholes.[7]

RCN, AT&T, and TWC (the commercial respondents) rely on the same exemptions as DOITT and ECS in their answers. In their joint memorandum, they reject Professor Crawford's

[7] ECS also argues res judicata and statute of limitations, but the Court rejected these arguments in its earlier ruling.

argument that high risk targets can be secured by the redaction of information about high risk targets, stating that "[t]he communications network itself is a high risk target." Intervenor's Mem. in Opp., p.6. They refer to an FCC study on the security of manholes, which notes that vandals who have accessed communications systems by opening manhole covers have caused outages. They additionally cite to a number of news stories which they annex, and which recount instances in which vandals "or others" destroy parts of the communications infrastructure and concomitantly cause widespread outages. They note that in Rankin v. Metropolitan Trans. Auth., Index No. 101127/2010 (Sup. Ct. N.Y. County Aug. 10, 2010) (avail at 2010 WL 3285633) (Rankin II), a justice in this county held that detailed New York City subway blueprints, which included detailed descriptions of both the subway system and the station layouts and which could not be redacted, were excludable under the life or safety exemption. They state that, utilizing the same reasoning, conduit information should be exempted here.

In addition to the alleged dangers to which DOITT and ECS refer, the commercial respondents argue the information constitutes propriety information subject to the trade secret exemption, which exempts trade secrets as well as information that, if publicly available, would harm their competitive positions with respect to each other and to additional communication service providers. They note that the exemption applies if the information constitutes a trade secret or it would result in a substantial competitive injury if released. Quoting Marietta Corp. v. Fairhurst, 301 A.D.2d 734, 738 (3rd Dep't 2003) (citations and internal quotation marks omitted, they state that to determine whether something constitutes a trade secret a court must consider

> (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.

The commercial respondents argue that they have shown these elements. They emphasize that while each of them knows "the precise location and extent of its own facilities within ECS conduit, they do not have that same information about one another's facilities." Id., p.1. They state the conduit information is protected as a trade secret because it is the result of their work compiling evidence and making financial and strategic decisions concerning their routes. They state that they have invested substantial funds as well as time developing, building out, and marketing their networks. They contend that they treat the information as confidential and have worked to protect its confidentiality, often requiring those who receive it to sign nondisclosure agreements and only allowing properly credentialed employees access to the information. In support they point to the affidavits of Noel Dempsey of TWC and Christopher F. McDermott of AT&T, both of which speak about these protective measures.

The commercial respondents also reject Professor Crawford's argument that much of the information she seeks is already publicly available. Only a few ECS customers have shared their routes with the public, they state, and the commercial respondents are not among them. Moreover, they argue that the public maps are not very detailed and do not provide information about the manholes and conduits underneath them. Discussing the monetary value of the information, they cite the Dempsey affidavit, which states that TWC has spent hundreds of millions of dollars on market research to determine where to expand service to commercial entities and well over one hundred million dollars expanding its network to residential areas. He states that

the information Professor Crawford seeks would give TWC's competitors access to their research for free and also would tell them where TWC plans to expand its services so they can expand their own networks in these areas before TWC has the chance to do so itself.

Charmaine Stradford, the director of AT&T's project marketing management, notes that the more than fifteen companies who have cable franchises in New York City are highly competitive with each other and conduct expensive market research to construct buildout plans and otherwise maintain their competitive advantages. She concedes that the franchisees could determine which manholes contain AT&T's – or another provider's – conduit routes without the unredacted lists at issue here, but states it would require a lengthy and costly examination of the 10,530 manholes in the city. She states the unredacted list would reveal redundancies (duplicate conduit providers have in case a communications breakdown occurs) and thus enable competitors to learn the areas in which others provide faster, more direct routes and exploit this knowledge. She notes that AT&T provides sophisticated services to high-paying customers by the use of Ultraavailable Network Service (UVN) rings. Disclosure of full conduit information, she claims, would enable competitors to determine the identity of AT&T's high-paying clients and then enter through the pertinent manholes, explore the bandwidth capacity and characters of the data transmitted – and, if applicable, tell those customers the ways in which their services are superior.

In reply, Professor Crawford reiterates that even if some of the disclosure might cause harm to the telecommunications network, this does not justify a wholescale exemption of the material she seeks. She distinguishes the spreadsheet from the maps in that the former, unlike the latter, is redactable. She repeats that DOITT has numerous ways in which it can fulfill its

responsibility. It can provide conduit information for specific areas, limited by zip code or residential neighborhood, for example, or redact the spreadsheet so as to reveal only the endpoints of vacant conduit – which, she contends, does not jeopardize the security of any future tenants, and does not pose a current security threat. Further, she states, "the hypothetical and attenuated incremental risk of harm" does not require application of the exclusion, particularly in light of the fact that "significant information about telecommunications infrastructure . . . is routinely made public." Crawford Reply Mem., p. 3. Because DOITT has not tried to segregate the sensitive information but instead withheld everything she needs for her study, she contends, its decision is arbitrary and capricious.

Additionally, Professor Crawford points out, to invoke the IT exemption respondents must show that the security of the IT assets would be jeopardized. Even if respondents can make such a showing, moreover, the exemption must be applied narrowly. She claims that the commercial respondents are incorrect that the entire communications network is a high-profile target, because this interpretation of the IT exemption would allow DOITT to exclude almost all aspects of its regulation of the infrastructure. Moreover, plaintiff claims, respondents have not shown that disclosure increases the risk to the IT network as a whole, as terrorists and vandals could easily target the manholes in areas with "high value targets." Crawford Reply Mem., p.4. She argues that respondents' attempts to rely on Crawford I for the principle that the entire communications network is exempt is misplaced. In fact, she claims, the earlier litigation undercuts their position, because Justice Hagler conducted an in camera review to determine whether sensitive information could be redacted from the map. If the entire network were excludable, Professor Crawford points out, there would have been no need to conduct this review.

Professor Crawford states that respondents' three proffered arguments against disclosing limited data lack merit. First, she says, disclosure of conduit information in underserved communities does not put these communities at higher risk of losing services because "proper redactions to the database can largely eliminate the risks they cite, such as damage to key government agencies." Id., p.6. Second, if DOITT provides the spreadsheets for specific neighborhoods and redacts high profile targets, it will not be possible for anyone to use the data to reconstruct the map petitioner requested in Crawford I. Because the city's emergency services contain redundancies to safeguard against vandalism or terrorism, and because most people use their cell phones to call 911, the potential for total disruption of these services is minimal. She further notes that "the locations of cell antennas themselves are a matter of public record." Id., p.7. Third, she finds the argument that low-risk targets may turn into high-risk targets in the future to be "wildly speculative" and conclusory, and states that it does not relieve DOITT of its obligations under FOIL.

Next, petitioner claims that the life or safety exemption is inapplicable. Under that exemption, records which "could endanger the life or safety of any person" should not be disclosed. POL § 87(2)(f). According to petitioner, respondents simply have reiterated their arguments concerning the IT exemption, claiming they apply here as well, and have asserted in conclusory fashion that the lives and safety of those who work in or near manholes will be in jeopardy. Respondents' contentions, petitioner claims, are merely speculative, and moreover do not establish that a causal connection exists between disclosure and the asserted dangers. She claims that the existence of a generalized risk of terrorism is insufficient unless respondents show

there is a nexus between the disclosure and the criminal acts that may transpire. More specifically, she argues that respondents have not shown the alleged risk of damage to conduits could cause a loss of human life – only the temporary loss of connectivity. She claims that the cases upon which respondents rely – Asian Amer. Legal Defense & Educ. Fund v. N.Y. City Police Dep't, 125 A.D.3d 531 (1st Dep't 2015), lv denied, 26 N.Y.3d 919 (2016); Grabell v. N.Y.C. Police Dep't, 139 A.D.3d 477 (1st Dep't 2016); and Rankin II, Index No. 101127/2010 (Sup. Ct. N.Y. County Aug. 10, 2010) (avail at 2010 WL 3285633) – involved either information about counterterrorism practices or information that, following disclosure of similar situations in other geographic areas, had led to attacks. Here, on the contrary, respondents do not provide any "example of internet infrastructure targeted in a way that directly caused damage to an individual's life or safety." Crawford Reply Mem., p.11. Further, as with their arguments in support of the IT exclusion, petitioner claims, respondents have ignored their responsibility to consider the possibility of "partial disclosure and careful redaction" which could eliminate the "speculative harm." Id.

Disclosure also is appropriate here, Professor Crawford reiterates, because much of the information is already public, and she adds that this is at least partly due to the interest in eliminating the "digital divide" between the underprivileged and the middle and upper classes. She asserts that there is some granular data available publicly, such as maps showing where high-speed service exists in Bronx Community District 1 and Manhattan Community District 8; and that California, for example, provides a map which "shows where conduit exists, who occupies the conduit, and even what type of wires are used." Id., p.16. Even in New York City, she points out, twelve small broadband providers have made their data public.

Professor Crawford further contends that the trade secret exemption does not apply. She argues, on this issue, that ECS, which controls and rents space in the conduits, created the spreadsheet and has not asserted that it is a trade secret. Further, she states, though it currently might be costly or burdensome to determine where the ECS conduit runs, this does not mean that cable providers which rent from ECS can shield all locational information from the public. She claims the information at issue does not fall within the scope of a trade secret because its disclosure would not enable competitors to obtain an advantage over the commercial respondents. She points out that the fiber is tagged and therefore any provider who accesses the manhole can identify all the other providers that access it. Thus, the information is not actually secret. She contends that the mayor's office has compiled and released granular data about high-speed internet access and that the New York City Department of Transportation's (DOT) public, interactive map shows what work permits DOT has granted for work in the manholes, enabling citizens to "readily ascertain the location of all active street permits held at any time by any of the intervenors." Id., p.19. Petitioner dismisses the commercial respondents' position that if their locational information is disclosed their competitors can exploit it. She states that in Markowitz v. Serio, 11 N.Y.3d 43 (2008), the Court of Appeals rejected a similar argument on the ground that it was too speculative.

In addition, she argues, the commercial respondents cannot satisfy the alternative prong of the exemption, which requires a showing that disclosure of the spreadsheet would cause "substantial injury" to their competitive positions. POL § 87(2)(d). She contends that only ECS can assert this exemption and only on its own behalf, as it created the spreadsheet using information from its own records. Moreover, ECS, which has a monopoly, cannot assert competitive harm. Furthermore, she argues, the commercial respondents cannot show that they

will suffer substantial competitive harm due to the disclosure. She states that pursuant to Encore College Bookstores, Inc. v. Ausiliary Service Co., 87 N.Y.2d 410, 420 (1995) (Encore Books), courts must balance the value of the disclosure against any damage that may arise, and here the balance weighs in favor of allowing for the limited disclosure.

On April 4, 2017, the parties orally argued this motion before the Court, on the record. They debated whether petitioner had to submit a new FOIL request with her pared-down demand rather or could suggest modifications to her request in the course of the litigation. Petitioner described the conflicting ways in which the parties define "underserved neighborhoods," id., p. 14, ll.22-23, and stated that because of this conflict the parties would not be able to resolve their conflict in a new FOIL proceeding. She stated she does not seek information that would reveal the routes of conduit once they went outside of these areas.

Additionally, DOITT claimed that for security reasons even people in the mayor's office and the broadband taskforce are not provided full access to infrastructure information while they work on ways to improve the system. Further, it stated, information about vacant conduits also must be withheld as they are part of the infrastructure. It stated that the possibility that "innocuous" information might become important is sufficient to justify exemption of the entire network. It contended that 911 calls by cellphone rely on conduit wires for part of their routes. DOITT distinguished New Jersey and California's publicly available broadband maps in that they allegedly only show where there is broadband access or other types of service.

AT&T stated that petitioner's suggested modifications do not reasonably describe "underserved communities," the information she seeks. Turning to trade secrets, AT&T argued that disclosure of the spreadsheet would reveal "strengths about where to invest and how much to invest." April 4, 2017 Transcript, p.48, ll.13-14. TWC added that the information as to where the respondents are "rolled out" and "not rolled out" is extremely critical, especially in relationship to the "titanic battle[]" between FIOS and cable. Id., p.50, ll.1-3. It contended, as to IT exemption, that information about "switching hubs," through which a company runs numerous cables, could be used to wreak maximum havoc to that provider's network.

"The purpose of FOIL, found in article 6 of the Public Officers Law, is to shed light on government decision making, which in turn both permits the electorate to make informed choices regarding governmental activities and facilitates exposure of waste, negligence and abuse." Encore Books, 87 N.Y.2d at 416 (citations omitted). Accordingly, "a broad standard of open disclosure" applies, and all records are disclosable unless a specific statutory exemption applies. Id. at 416-17. Agencies opposing disclosure under FOIL bear "the burden of demonstrating that the requested material falls squarely within a FOIL exemption by articulating a particularized and specific justification for denying access." TJS, 89 A.D.3d at 241 (citations and internal quotation marks omitted); see Abdur-Rashid v. New York City Police Dep't, 140 A.D.3d 419, 421 (1st Dep't 2016) (requiring a "detailed affidavit" establishing the applicability of the exemption). Furthermore, in reviewing a FOIL determination in the context of an Article 78 challenge, courts apply a less deferential standard, deciding whether decisions were "affected by an error of law" rather than whether they were "arbitrary and capricious." See Mulgrew v. Bd. of Educ. of City Sch. Dist. of City of N.Y., 87 A.D.3d 506, 507 (1st Dep't 2011) (quoting CPLR §

7803(3)); see also Verizon New York, Inc. v. New York State Public Serv. Comm., 137 A.D.3d 66, 69 (3rd Dep't 2016) (Public Serv. Comm.) (courts "need not accord any deference to the agency's [FOIL] determination").

Initially, the Court addresses respondents' argument that petitioner cannot modify her FOIL demand to include conduit information only for underserved communities and unused conduit in these areas. In this, respondents echo DOITT's March 12, 2015 decision, which rejected this suggestion on the ground that she "assume[d] that the records access counsel was obligated to interpret your request to be other than as you stated it." DOITT Appeal Determination, March 12, 2015, p.2. Respondents are incorrect. While it is true that she cannot revise her FOIL request during the Article 78 appeals process, thus bypassing the necessary formal DOITT consideration of the revision, it is not petitioner's burden to pare down her request. Instead, as she correctly notes, DOITT has the sole burden of showing why the information it has withheld should be excluded. County of Suffolk v. Long Island Power Auth., 119 A.D.3d 940, 942 (2nd Dep't 2014). Moreover, it is DOITT's responsibility to provide redacted documents which include as much information as possible to fulfill petitioner's request. See Data Tree, LLC v. Romaine, 9 N.Y.3d 454, 462 (2007) (Data Tree). In addition, this Court must review the legal basis for DOITT's actions and determine whether, based on petitioner's arguments, DOITT can hand over some or all of the information petitioner has requested. In so doing, the Court must narrowly interpret the so that the public is granted maximum access to the records of government. See id. at 454. Thus, the Court can take into account any suggestions petitioner has presented in the hope of settling or successfully resolving this dispute. See The Empire Center for Public Policy, Inc. v. NYC Office of Payroll Admin., Index No. 100079/2016, at *3 (Sup. Ct. N.Y. County Jan. 18, 2017) (avail at 2017 WL

403099) (court adopted petitioner's suggestion in determining how materials could be meaningfully redacted); Rankin v. City of New York Dep't of Information Technology and Telecommunications, Index No. 109626/2008 (Sup. Ct. N.Y. County Jan. 28, 2009) (Rankin I) (pursuant to the parties' stipulation, the court limited its review to the FOIL request as modified by petitioner).

Next, the Court considers the question of whether the IT exemption applies. The applicable provision, POL § 87(2)(i), states that if materials, "if disclosed, would jeopardize the capacity of an agency . . . to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures." POL § 87(2)(i) (quoted in TJS, 89 A.D.3d at 243). As petitioner notes, this issue has not been litigated often in the courts of New York. In addition to Crawford I, the parties discuss TJS. This proceeding involved a request for information about a tax audit. The respondent argued that the data could not be reviewed without the department's software and that the software, in turn, was excludable under the IT exemption. The court rejected the respondent's argument – that those who acquired the software could breach or compromise the department's IT infrastructure or use the information to manipulate data – ruling that these statements were not sufficient to show the exclusion applied. TJS, 89 A.D.3d at 243.

As stated, the Court's role in evaluating this and respondents' further arguments is to decide whether DOITT's determination was affected by an error of law. Mulgrew, 87 A.D.3d at 507. Moreover, it bore the burden of supporting its numerous redactions to the document in a detailed fashion and explaining why proposed modifications were unacceptable. The Court

concludes that DOITT failed in both respects. The Court accepts for the sake of argument that conduit routes are included in the IT exemption. Also, as respondents contend, information technology is increasingly important as a means of communication in the twenty-first century. Indeed, it is in part because of this fact that petitioner argues high-speed internet access should be available in all communities and contends her research is important. In addition, as respondents point out, since September 11, 2001, the country has been more aware of its vulnerability to terrorism. The Court is cognizant of the concerns expressed in the affidavits of Chief Waters, Christopher F. McDermott, and Noel Dempsey, among others, relating to the publication of the entire communications infrastructure. If anyone could reconstruct the routes in their entirety, this would create a danger that high risk or high traffic portions of the IT network could be targeted with greater ease.

It does not follow, however, that all of the information in the spreadsheet should be redacted when it is possible to provide petitioner with the data she needs for her research without jeopardizing the security of the infrastructure. Crawford I, which respondents cite for support, categorizes the conduit as part of the infrastructure, see Crawford I, 43 Misc. 3d at 740-41, but expressly leaves open the possibility that some information is nonetheless disclosable. See id. at 744. As petitioner correctly notes, this actually undercuts respondents' argument on this issue. Moreover, petitioner's suggestions – to exclude information about the routes leading to high profile targets and about switching hubs, and to focus on unused conduit in underserved communities – would vitiate the dangers to which respondents, and in particular DOITT and ECS, refer. The affidavits of Chief Waters and others do not mention or assess the possible danger of providing the spreadsheets as limited. Respondents' argument that all of the network must be

excluded is unpersuasive in a situation like the one at hand, where the information is segregable. Therefore, respondents have not satisfied their burden.

There is always a risk that vandals or terrorists can disrupt the communications network by lifting ECS manhole covers and cutting cables which run through the conduits. Bad weather and problems with the cables themselves also cause outages periodically without the intervention of vandals or terrorists; one critical study respondents provide discusses the telecommunications problems that occurred in the aftermath of Superstorm Sandy. Several other annexed studies, including one relating to the security of manhole covers, suggest making the manhole covers themselves more secure so would-be intruders cannot open them. Other suggestions are that cable service providers should monitor access to the covers, develop network resiliency through redundancies in the network, that additional alternate routes be created, and develop advance, detailed planning for recovery from outages. Moreover, respondents acknowledge that several smaller cable providers have made information including their routes available to the public, yet they have not argued that the publication of this data has resulted in damage to those providers' cables or otherwise has compromised infrastructure security. Respondents have not shown that disclosure of the spreadsheet, with the suggested redactions, will appreciably increase the existing risk.

Respondents' second argument is that "if disclosed [the information] could endanger the life or safety of any person." POL § 87(2)(f). Because of the importance of FOIL's underlying principle of open government, the agency seeking this or any exemption must "articulate [a] particularized and specific justification for not disclosing requested documents."

Gould v. New York City Police Dep't, 89 N.Y.2d 267, 279 (1996). This does not mean that the agency must establish that danger necessarily will result from the disclosure. Instead, it must show that a real possibility of endangerment exists. Bellamy v. The New York City Police Dep't, 87 A.D.3d 874, 875 (1st Dep't 2011). In practice, this exclusion has been applied where, for example, the petitioner requests the identity of undisclosed witnesses who have cooperated in the investigation of a gang-related murder, id., or an attempted murder-by-shooting. The Exoneration Initiative v. The New York City Police Dep't, 114 A.D.3d 436, 439 (1st Dep't 2014).

With respect to this exemption, too, respondents have not satisfied their burden. In addition to the arguments which the Court already has discussed in connection with the IT exemption,[8] respondents argue that people may be endangered if there are outages that involve those cables that connect to hospitals and other sites which provide critical services to individuals. They note that the risk also exists in underserved communities. Petitioner's suggestion to exclude information about these critical parts of the network, however, would obviate this concern. Respondents have not countered her suggestion or stated that this redaction is impossible. Similarly, redundancies and the general availability of cell phones dramatically reduce the risk that individuals will be unable to access 911. Further, since September 11, 2001, to which respondents have referred in support of their arguments, state and federal authorities have taken numerous steps to minimize the risk of losing 911 services and critical care services in the event of an emergency that affects the communications system. The chance that there might be people at work in the

[8] As petitioner states, many of respondents' arguments here replicate those they raise with respect to the IT exemption. This is not surprising, as the issues of the security of technology and of the IT infrastructure are increasingly intertwined with that of the safety of the public.

manholes at the precise time terrorists or vandals invade the manholes, and that the terrorists or vandals might harm these workers, is too hypothetical and remote to justify the exemption, and does not noticeably increase the existing risk to these workers. Respondents have not adequately established that the exemption is justified in light of the reduced discovery petitioner now seeks.

Respondents point to three cases in support of their argument that the exemption applies here. All are distinguishable from the situation at hand. Grabell v. New York City Police Dep't, 139 A.D.3d 477 (1st Dep't 2016), and Asian-American Legal Defense and Educ. Fund v. New York City Police Dep't, 125 A.D.3d 531 (1st Dep't 2015) (Legal Defense Fund), lv denied, 26 N.Y.3d 996 (2016), involved requests for material specifically related to the police department's antiterrorism efforts – in Grabell, the locations and past locations of vehicles containing equipment that can detect bomb-making devices and drugs; and in Asian-American Legal Defense and Educ. Fund, materials describing police department intelligence operations.[9] The risks attendant upon disclosure were direct rather than attenuated.

Third, respondents analogize the matter at hand to Rankin II, Index No. 101127/2010 (Sup. Ct. N.Y. County Aug. 10, 2010) (avail at 2010 WL 3285633). In Rankin II the petitioner sought a detailed map of all of the city's subway stations, including the locations of stairways, elevators, attendant books, and vending machines (the blueprint). Rankin II is more analogous to the FOIL demand in Crawford I, which involved a map for which simple redaction

[9] The FOIL request in Asian-American Legal Defense and Educ. Fund was deemed too vaguely worded to enable the agency to comply, but the court discussed the above arguments in the alternative.

was impossible without creating a new document. Here, on the other hand, redaction is possible and is not onerous.

Respondents finally rely on POL § 87(2)(d), which exempts trade secrets which a commercial enterprise provides to an agency, and materials the agency prepares based on information that a commercial enterprise has provided which would cause "substantial injury to the competitive position" of the commercial enterprise if disclosed. As the commercial respondents stress, these are two separate exemptions; if the Court decides the material in question is a trade secret, they need not show substantial competitive injury. See Public Serv. Comm., 137 A.D.3d at 68. On the issue of trade secrets, courts initially consider whether the material is "a formula, pattern, device or compilation of information" the commercial entity uses to its competitive advantage. Id. at 72 (quoting New York Telephone Co. v. Public Serv. Comm. Of the State of New York, 52 N.Y.2d 213, 219 n.3 (1982)). If so, courts next consider various additional factors, 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.

Schroeder v. Pinterest Inc., 133 A.D.3d 12, 27 (1st Dep't 2015) (in commercial dispute involving alleged misappropriation of trade secrets).

After careful consideration, the Court concludes that the spreadsheet is not a trade secret within the meaning of the statute. Although the commercial respondents compile data when they research where to lease conduit space, where to run their cables currently, and where to retain the space for future use, it is not this data which is at issue, but the conduit they decided to lease after studying and compiling the information. Moreover, respondents cannot satisfy the remainder of the factors. For one thing, the cables inside the conduits are tagged to identify the owners so they know which wires to access for maintenance and other purposes. Therefore, this information is ascertainable to employees for all of the commercial respondents, to other lessees of the conduit in question, and to anyone else who accesses the manholes for any reason. Although petitioner has overstated the amount of this information that is already available to the public, she has shown that several smaller providers have shared information about their routes on public sites, and that some state governments and the federal government have released broadband maps which include, albeit not on a granular level, the availability of cable in various neighborhoods. Thus, some, if not all, of the information is more easily available. Finally, and significantly, the information in the spreadsheet is not secret. Indeed, in her affidavit on behalf of the commercial respondents, Charmaine Stradford of AT&T conceded that franchisees can determine the conduit routes of their competitors without the spreadsheet, albeit by dint of significant effort. Also, as this Court noted at oral argument, the information about which neighborhoods have higher speed cable service from each provider and which have limited, substandard, or no cable access is not secret.

The commercial respondents have shown that they view their conduit routes as proprietary and valuable, and that they work to keep the information secret. The Dempsey affidavit on behalf of TWC and the Stradford affidavit which AT&T has submitted both explain the lengths

to which they go to maintain this privacy – requiring DOITT to note their confidential nature, for example, and providing nondisclosure agreements to those who access their cables. In addition, they have spent time and a great deal of money to develop the information, although they have not set forth concrete information about these expenditures. The facts that these respondents want the information to remain secret and that they have worked to maintain its secrecy, however, are not enough to transform otherwise discoverable information into a trade secret.

Sunset Energy Fleet L.L.C. v. New York State Dep't of Environmental Conserv., 285 A.D.2d 865 (3rd Dep't 2001) (Sunset Energy) illustrates this point. Sunset Energy involved an air quality and pollution study by the petitioner which it prepared in order to obtain approval for the construction of a 520 megawatt electric generating facility. The petitioner's detailed study allegedly cost over 2,200 work hours and around $225,000 – a relatively high cost for a single facility. The Third Department determined that "the compiled information in the worksheets" did not qualify as a trade secret simply because the "petitioner had to compile, verify and analyze the [publicly available] data." Id. at 867. In addition, it noted that the despite the time and expense of the project, the resulting work could be reproduced using the same data. Here, the commercial respondents' data was not compiled using known a fixed methodology. This distinction is not dispositive, however. The methodology the commercial respondents used to determine where to lease conduit space and where and when to build out cables may constitute a trade secret, but the spreadsheet petitioner seeks here does not reveal either the methodology or the research.

The second prong of POL § 87(2)(d) protects enterprises which can show they will suffer "a significant competitive injury as a result of disclosure of information it provided to the agency." Verizon New York, Inc. v. Bradbury, 40 A.D.3d 1113, 1115 (2nd Dep't 2007) (emphasis supplied). To show competitive injury, "the part[ies] seeking the exemption must present specific, persuasive evidence that disclosure will cause it to suffer a competitive injury; it cannot merely rest on a speculative conclusion that disclosure might potentially cause harm." Markowitz v. Serio, 11 N.Y.3d 43, 51 (2008). Where the harm is theoretical, therefore, the respondents have not satisfied their burden. Id.

The commercial respondents have not satisfied their burden of showing that this exemption applies. Instead, the damage they assert is hypothetical. Encore Books, 87 N.Y.2d 410, upon which the commercial respondents rely, does not mandate a different outcome. In that case, the owner of a bookstore previously "suffered a significant decrease in sales revenue" following the release of the same material for prior years. Thus, "the likelihood of substantial competitive injury" was apparent. Id. at 421. Here, on the other hand, the commercial respondents have not pointed to any specific data showing that it would likely suffer substantial injury – by showing, for example, that the publication of their conduit routes harmed the smaller providers, or that this type of disclosure has resulted in substantial competitive injury in those states which make more information available to the public. Further, petitioner notes that she has suggested limiting the disclosure in a manner which limits this alleged competitive harm so that it is not substantial. In response, the commercial respondents have not shown they will suffer substantial competitive injury if the spreadsheet is redacted pursuant to petitioner's suggestions. In fact, they have not addressed the question due to their insistence that all of the information must be redacted.

The primary injury the commercial respondents allege here is that other companies might look at the conduit routes, see where providers have leased space and which of this leased space is unused, and then take advantage of their competitors' weaknesses and gaps. In Markowitz the Court of Appeals rejected a similar argument as insufficient. Markowitz, 11 N.Y.3d at 51.[10] In an appeal to the New York Public Service Commission (PSC),[11] TWC and Comcast Corporation raised a similar argument with respect to the disclosure of proposed build-outs. Joint Petition of Time Warner Cable Inc. and Comcast Corporation for Approval of a Holding Company Level Transfer of Control. Appeal of an Administrative Law Judge's FOIL Determination, Case 14-M-0183 (Jan. 9, 2015) (avail at 2015 WL 164710 (N.Y.P.S.C.)) (Joint Petition). In ruling against TWC and Comcast, the Commission found that the argument that if information related to "where and when TWC planned to deploy broadband, competitors would be able to upgrade their services . . . before [TWC] even completed its deployments" was not compelling because "TWC does not provide any specific evidence or details about the nature or extent of the competitive advantages it alleges will be lost." Id., 2015 WL 164710, at *9. For similar reasons to those in Markowitz and Joint Petition, the Court finds the commercial respondents have not satisfied their burden here.

Aurelius Capital Management, LP v. Dinalo, Index No. 108462/2008 (Sup. Ct. N.Y. County Jan. 13, 2009) (avail at 2009 WL 367770) (Aurelius), aff'd, 70 A.D.3d 467 (1st Dep't 2010). another case to which the commercial respondents cite, is also distinguishable. In that case,

[10] The argument was "that if they are forced to reveal [information relating to areas where the insurance companies have issued] relatively few policies ..., competitors could use this information to exploit an insurer's geographic weakspot."
[11] The Court is not bound by PSC's rulings but can look to them for guidance. Cf. Thomas v. New York City Dep't of Educ., 103 A.D.3d 495, 498 (1st Dep't 2013).

the court found the exemption applied in part because the business "established ... that [it] would be less able to compete for new business if prospective insureds learned that [it] could not maintain confidentiality ...." Aurelius, 2009 WL 367770, at *3. In addition, the court emphasized, the party seeking the information was a private business entity which wanted to increase its own business at the expense of another business entity. In this, it differentiated the case from Markowitz, in which a government official was conducting an industry-wide investigation. To the extent that the Aurelius Court considered the relative public interest which generates a FOIL request to be a factor in the FOIL analysis, it supports petitioner's position, as she seeks the information for a study she hopes will result in increased access to high-speed internet in lower-income communities.

The commercial respondents also cite James, Hoyer, Newcomer, Smiljanich & Yanchunis, P.A. v. State, Office of Atty. Gen., Index No. 114284/2009 (Sup. Ct. N.Y. County March 31, 2010) (avail at 2010 WL 1949120) (James, Hoyer), in which agency records relating to the government's investigation of the student loan industry were deemed to be exempt from disclosure. This case also is distinguishable. The James, Hoyer Court concluded that, among other things, disclosure would enable the law firm seeking the records "to learn customized information about the terms of SLM's[12] produce and service offerings to the client, including rate, benefits, counterparties and eligibility criteria." Here, on the contrary, petitioner seeks a spreadsheet which does not contain the type of customized information at issue in James, Hoyer, but information concerning the public routes developed using confidential information.[13]

[12] SLM was formerly known as Sally Mae.
[13] The court found additional exemptions applicable as well.

The commercial respondents reiterate that they have spent a great deal of money conducting research aimed to determine where they should lease conduit space. Every company in this case, and every other cable provider, also spend time and money to conduct this research, however, and they will continue to do so regardless of the outcome of this litigation. See Sunset Energy, 285 A.D.2d at 282. It is not clear the research and the tools the researchers use will be extremely different from one company to the next or that one company would adopt a competitor's strategy over its own. Most important, the disclosure as redacted will enable the commercial respondents to maintain the privacy of the majority of their conduit routes, including the customized network solutions (UVN rings) AT&T uses for its high-value customers.

The commercial respondents argue that petitioner's proposed compromise is unacceptable because petitioner and respondents disagree on the definition of "underserved." Petitioner states that an underserved community consists of "geographic areas in which less than 30% of the households subscribe to high speed internet access." April 4, 2017 Transcript, pp.14-15, ll.24-1. DOITT's working definition includes "areas that have systemic barriers to broadband penetration that go beyond mere lack of facilities." Id., p.15, ll.4-6. This dispute does not render disclosure impossible. Instead, the Court determines that petitioner's definition shall apply, as this is a rational one which will provide her with the discrete disclosure she needs.

Though the commercial exemptions exist to protect business interests, they do not exist to enable service providers to avoid competition. Often, therefore, "[c]ourts deciding FOIL issues ... order redaction when a record contains both exempt and nonexempt information." Schenectady County Soc. For the Prevention of Cruelty to Animals, Inc. v. Mills, 18 N.Y.3d 42,

46 (2011). Here, it is possible to provide redacted information which discloses the information petitioner requests, limited to underserved communities and unused conduit space in those communities, and excluding information relating to hospitals and other emergency service providers. The Court has considered all of the parties' arguments even if it has not discussed them.

Finally, in its discretion, the Court denies attorney's fees. Under Public Officers Law § 89(4)(c), "[t]he court . . . may assess, against such agency involved, reasonable attorney's fees and other litigation costs reasonably incurred by such person in any case under the provisions of this section in which such person has substantially prevailed, when: i. the agency had no reasonable basis for denying access; or ii. the agency failed to respond to a request or appeal within the statutory time." Quoted in Acme Bus Corp. v. Cty. of Suffolk, 136 A.D.3d 896, 897 (2nd Dep't 2016). Although petitioner has prevailed, she adjusted her demands significantly based on the security concerns on which DOITT based its denial. Therefore, the Court cannot conclude that she "substantially prevailed" or that the agency lacked a good faith basis for denying the disclosure petitioner sought.

Therefore, it is

ORDERED that the petition is granted to the extent that within 30 days, DOITT shall provide petitioner with a spreadsheet limited to the underserved communities as defined by petitioner, which redacts high-risk endpoints and switching hubs but includes the location of the

manholes, the number of tenants using each conduit, and the names of the commercial providers which rent space; and is otherwise denied.

Dated: May 11, 2017

ENTER:

JOAN B. LOBIS, J.S.C.