Decision 20-12-021 December 17, 2020

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking to Evaluate Telecommunications Corporations Service Quality Performance and Consider Modification to Service Quality Rules.	Rulemaking 11-12-001

DECISION ADDRESSING CARRIERS' CONFIDENTIALITY CLAIMS RELATED TO NETWORK STUDY ORDERED IN DECISION 13-02-023, AS AFFIRMED IN DECISION 15-08-041

TABLE OF CONTENTS

Title **Page**

DECISION ADDRESSING CARRIERS' CONFIDENTIALITY CLAIMS RELATED TO NETWORK STUDY ORDERED IN DECISION 13-02-023, AS AFFIRMED IN DECISION 15-08-041

Summary

This order addresses the confidentiality claims of Pacific Bell Telephone Company dba AT&T California and Frontier California, Inc. (formerly, Verizon California, Inc.) concerning information both telephone corporations submitted to the California Public Utilities Commission (Commission) as part of the Network Study ordered in Decision (D.) 13-02-023 and affirmed in D.15-08-041.

Pursuant to these decisions, an investigation into the service quality of California's two largest telecommunications networks was conducted by the Commission's Communications Division and Economics and Technology, Inc., an independent consultant whose services the Commission obtained for this purpose. The study focused on examining the telecommunications network infrastructure, facilities, policies, and practices of these two carriers, the results of which would inform future Commission action. The results of the Network Study are detailed in a report entitled "Examination of the Local Telecommunications Networks and Related Policies and Practices of AT&T California and Frontier California – Study conducted pursuant to the California PUC Service Quality Rulemaking 11-12-001, Decision 13-02-023, and Decision 15-08-041" ("Network Report" or "Report"), which has been entered into the record of this proceeding under seal pending the Commission's resolution of these carriers' confidentiality claims.

For the reasons stated in this order, we find that the Network Report should be made public, except for certain information that, if disclosed, could pose a security risk. We direct staff to redact the portions of the Network Report

that contain information afforded confidential treatment pursuant to this order and to make that redacted version available to the public.

1. Background

1.1. Purpose of the Network Study

The California Public Utilities Commission (Commission or CPUC) has broad authority, and extensive responsibility, to regulate telecommunications providers in California to ensure Californians receive high-quality and reliable service.[1] The Commission's authority extends to telecommunications infrastructures and facilities telephone corporations use to provide service to Californians.

The Commission initiated this rulemaking proceeding in response to a Communications Division (CD) staff report, which found substandard results in service quality filings by carriers subject to General Order (GO) 133-C, which sets forth service quality standards for wireline telecommunication corporations. This rulemaking assessed performance standards in 2010 and was initiated to determine whether the GO 133-C standards were adequate and whether the Commission needed to adopt a penalty mechanism for substandard service quality performance.[2]

The Commission determined that obtaining the services of an independent consultant to perform an examination of the telecommunications carriers' infrastructure, investment, and manpower to improve service quality ("Network Study") was a "foundational activity" in this proceeding, in that "it would

---

[1] *See, e.g.*, Cal. Const., Art. XII; Pub. Util. Code §§ 313, 314, 314.5, 315, 451, 453, 582, 584, 701, 709, 761, 762, 768, 776, 792, 793, 2889.8, and 2896.

[2] Rulemaking (R.) 11-12-001, Order Instituting Rulemaking to Evaluate Telecommunications Corporations Service Quality Performance and Consider Modification to Service Quality Rules (OIR), at 3-4.

provide empirical data on the condition of network infrastructure, as well as on carrier infrastructure policies and procedures."[3] This data would "facilitate an examination of the quality of existing communications services, and potentially inform the development of new and improved metrics to measure service quality."[4] CD oversaw the consultant, Economics and Technology, Inc. (ETI), in the Network Study of the two principal wireline carriers in California: AT&T and Verizon (subsequently purchased by Frontier, hereinafter referred to collectively as "Frontier").[5]

In 2016, the Commission affirmed, over the carriers' objections, that the study should go forward because it could be used as a basis for future clarification and revision of the Commission's service quality rules.[6] Indeed, the Commission repeatedly confirmed that the study of AT&T and Frontier networks ordered in D.13-02-023 remained a "necessary"[7] and "foundational activity" because "[r]eliable, high-quality telecommunications services are crucial for the health of California's economy and the safety of California citizens."[8] The

---

[3] *Id*. at 15; *see* also D.13-02-023, at 2-3; *see* also D.15-08-041, at 11.

[4] *Id*. at 15; *see* also D.13-02-023, at 2-3; *see* also D.15-08-041, at 1, 7, 8-9, 10-11.

[5] Assigned Commissioner's Scoping Memo and Ruling, filed December 1, 2011 in R.11-12-001, at 12.

[6] *See* D.15-08-041 at 10; *see* also D.18-10-058 at 22-24.

[7] *See* D.15-08-041 at 2 *citing* Pub. Util. Code § 2889.8 ("The commission periodically shall assess the reliability of the public communications network and, if necessary, develop recommendations for improvement.").

[8] D.15-08-041 at 1, 7, 8-9, 10-11; *see* also *id*, Findings of Fact 2-6, Conclusions of Law 1-3; *see* also D.13-02-023 at 2-3 ("The scoping memo and ruling issued on September 24, 2012, found that '[i]n order to maintain acceptable levels of service quality for California customers, it is necessary to ensure that carriers have access to an adequate network of infrastructure,' and includes within the scope of this proceeding an evaluation of carriers' network infrastructure, facilities, and related policies and practices. …The purpose of this evaluation is to gauge the

Commission rejected industry claims that this Network Study was unnecessary in light of the penalty mechanism the Commission was considering, stating:

> …a penalty mechanism alone, even if related to meaningful metrics and standards, would not prevent the damage that could be caused by a network failure. Because of the central importance of network infrastructure in supporting emergency services, both to assist individual customers and to coordinate public sector response to a broader emergency, a communications failure could undermine public health and safety, which are core concerns of this Commission.[9]

The Network Study was completed in 2019.

1.2. The Network Study and Report

In April 2019, ETI produced the Network Report. In producing this 584-page report,[10] ETI relied upon a broad range of data, including information obtained from public sources and directly from the carriers. Principal among these data sources were eight categories of information:

- Category 1: Reports and raw data that AT&T, Verizon (prior to the transfer of its California ILEC operations to Frontier on April 1, 2016), and Frontier have been required to provide to the CPUC on an ongoing basis pursuant to General Order 133-C/D regarding customer trouble reports and the respective companies' responses thereto.
- Category 2: AT&T and Frontier responses to data requests submitted by ETI and by CPUC Communications Division staff.
- Category 3: Information and photographs CPUC staff obtained from site visits (e.g., outage locations; network

conditions of the carrier infrastructure and facilities … to ensure that the facilities and related practices support a level of service consistent with public safety and customer needs.").

[9] D.15-08-041 at 11 (citations omitted).

[10] The Network Report consists of 12 chapters. A public version of the Report's Table of Contents and other select chapters with preliminary redactions may be found at https://www.cpuc.ca.gov/General.aspx?id=6442462050.

facility maps; photographs of equipment inside AT&T and Frontier Central Offices).

- Category 4: Annual financial reports AT&T California, Verizon California, and Frontier California file with the CPUC that conform to the Federal Communications Commission's Automated Regulatory Management Information System (ARMIS) reporting requirements. While largely discontinued by the Federal Communications Commission (FCC) after 2007, the CPUC has continued to require these reports to be filed by Uniform Regulatory Framework Incumbent Local Exchange Carriers (ILECs).
- Category 5: Public financial data and disclosures obtained from annual, quarterly and special reports – 10-K, 10-Q and 8-K reports – as filed by the two ILECs' parent companies – AT&T Inc., Verizon Communications, Inc. and Frontier Communications, Inc. – with the Securities and Exchange Commission (SEC), as well as Annual Reports to Shareholders and other shareholder communications issued by the various parent companies.
- Category 6: Industry data and reports the CPUC and the FCC publish.
- Category 7: Statewide and county-wide industry data for California the FCC publishes.
- Category 8: Other government data sources, including the US Census Bureau, the Bureau of Labor Statistics, various California state agencies, and the National Oceanographic and Atmospheric Administration.

Categories 1 through 4 consist of information the carriers produced or gave to staff, with claims of confidentiality. This decision addresses these

confidentiality claims to the extent the information appears in the Network Report.[11]

Categories 5 through 8 consist of information obtained from public sources and thus are not at issue here.

1.3. August 16, 2019 Assigned Commissioner's Ruling Requiring Substantiation of Carriers' Confidentiality Claims

On August 16, 2019, the Assigned Commissioner issued an Assigned Commissioner's Ruling (ACR) that ordered AT&T and Frontier (the carriers) to file and serve statements substantiating the confidentiality claims the carriers made in submitting information on which the Network Study was in part based. The ACR noted that the Commission's Legal staff reviewed the carriers' confidentiality declarations and concluded that, because of the overly general nature of the objections raised, these declarations did not adequately set forth legal and factual grounds justifying confidential treatment of such information, as required in General Order 66-D.

The August 16, 2019 ACR provided the carriers another opportunity to provide specific legal and factual bases for confidential treatment of any Network Study information provided to the Commission and ETI, noting that failure to make such a showing would result in the disclosure of such information. The ACR entered the Report into the record under seal, pending resolution of the carriers' confidentiality claims.

---

[11] Categories 1 through 4 information described above are reflected in the Network Report chapters as follows: Category 1 information (GO 133-C/D Service Quality Reports and Raw Data) appears in chapters 1, 2, 4 (4, 4A, 4F); Category 2 information (Network Study Data Requests and Carriers' Responses) appears in chapters 1, 3, 5, 6, 9, 10; Category 3: Staff Site Visits) appears in chapters 1, 12; and Category 4 information (Annual Financial Reports, *i.e.*, ARMIS reports) appears in chapters 1, 7, 8. The confidential treatment of any contested information in Chapter 1 (Executive Summary and Overview) will be informed by this decision's analysis of Categories 1 through 4 as they appear in chapters 2 through 12.

1.4. The Carriers' Responses to the August 16, 2019 ACR

On September 3, 2019, AT&T and Frontier each filed a response to the ACR. Both carriers contend that most of the information from Categories 1 through 4 is confidential on various grounds, including that such information constitutes customer specific information, trade secrets, critical infrastructure information, financial information, or competitive information, which are protected from disclosure by state or federal laws.

Frontier states that it had difficulty responding to the ACR because neither carrier had an opportunity to review the Network Report to see how the Commission or ETI used the carrier-provided information in the Report.[12] While the Commission has yet to publish the entirety of the report, lightly-redacted versions of the report's Table of Contents and Chapter 1 were made available on the Commission's website prior to the ACR's issuance. Redacted versions of Chapters 2, 3, 4, and 11 were subsequently made available.

The Table of Contents states with specificity the subject matter of each chapter, including chapter subparts, and it also includes a detailed description of the tables and figures presented in each chapter. Moreover, Chapter 1 sets forth the "Executive Summary and Overview of This Report," which consists of a 38-page detailed description of each of the other 11 chapters.

The fact that the carriers had not seen the entirety of the Report should not have affected their ability to respond to the August 16, 2019 ACR, which asks the carriers to address the confidentiality of the *underlying data in the report – data that the carriers submitted in response to Network Study-related data requests or submitted as part of ongoing Commission-mandated reporting requirements*. The carriers already

[12] Frontier Response at 1.

had an opportunity to satisfy the requirements for confidential treatment when each submitted the information.[13] The August 16, 2019 ACR provided the carriers additional opportunity to substantiate their confidentiality claims.

This decision determines the public or confidential status of Category 1 through 4 information the carriers submitted that appears in the Network Report. This decision does not determine the status of any other information that the carriers provided to the Commission or ETI that does not appear in the Network Report, such as personally-identifiable subscriber information (*e.g.,* customer names, addresses, phone numbers, services purchased) or customer or incident-specific raw data underlying service quality reports.

2. Applicable Laws Related to Public Access to Government Records and Requirements for Confidential Treatment of Information Submitted by Utilities

Before we address the specific confidentiality claims AT&T and Frontier assert, we provide an overview of the general requirements and principles applicable to the disclosure of Commission records.

2.1. The Public's Right to Information

As the Commission has explained in numerous decisions, the public has a right to access most Commission records.[14] The California Constitution (Cal. Const.), Article I, § 3(b)(1) states:

> The people have the right of access to information concerning the conduct of the people's business, and, therefore, the

[13] *See* General Order 66-D.

[14] *See* e.g., D.20-03-014, *Decision on Data Confidentiality Issues Track 3*, at 10-13; *see* also D.17-09-023, *Phase 2A Decision Adopting General Order 66-D and Administrative Processes for Submission and Release of Potentially Confidential Information*, at 2-3, 9-12.

> meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny.[15]

Cal. Const., Article 3(b)(2) states that statutes, court rules, and other authority limiting access to information must be broadly construed if they further the people's right of access, and narrowly construed if they limit the right of access.[16] Rules that limit the right of access must be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.[17]

The California Public Records Act (CPRA) requires that public agency records be open to public inspection unless they are exempt from disclosure under the provisions of the CPRA.[18] "Public records" are broadly defined to include all records "relating to the conduct of the people's business"; only records expressly excluded from the definition by statute, or of a purely personal nature, fall outside this definition.[19] Since records received by a state regulatory agency from regulated entities relate to the agency's conduct of the people's

---

[15] *See e.g.*, *International Federation of Professional & Technical Engineers, Local 21, AFL-CIO v. Superior Court* (2007) 42 Cal.4th 319, 328-329.

[16] Cal. Const., Article 1, § 3(b)(2): "A statute, court rule, or other authority, including those in effect on the effective date of this subdivision, shall be broadly construed if it furthers the people's right of access, and narrowly construed if it limits the right of access. A statute, court rule, or other authority adopted after the effective date of this subdivision that limits the right of access shall be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest." (See, e.g., *Sonoma County Employee's Retirement Assn. v. Superior Court (SCERA)* (2011) 198 Cal.App.4th 986, 991-992.)

[17] *Ibid.*

[18] *Roberts v. City of Palmdale* (1993) 5 Cal.4th 363, 370 ("The Public Records Act, section 6250 *et seq.*, was enacted in 1968 and provides that "every person has a right to inspect any public record, except as hereafter provided." (§ 6253, subd. (a).) We have explained that the act was adopted "for the explicit purpose of 'increasing freedom of information ' by giving the public 'access to information in possession of public agencies.' "(*CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 651 [citation omitted]).")

[19] *See e.g.*, *Cal. State University v. Superior Court* (2001) 90 Cal.App.4th 810, 825.

regulatory business, the CPRA definition of public records includes records received by, as well as generated by, the Commission.[20]

The Legislature has declared that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[21] An agency must base a decision to withhold a public record in response to a CPRA request upon the specified exemptions listed in the CPRA, or a showing that, on the facts of the particular case, the public interest in confidentiality clearly outweighs the public interest in disclosure.[22]

The CPRA favors disclosure, and CPRA exemptions must be narrowly construed.[23] Unless a record is subject to a law *prohibiting* disclosure, CPRA exemptions are permissive, not mandatory; and thus, while the CPRA exemptions allow nondisclosure, they do not prohibit disclosure.[24] This means

---

[20] *See* Gov. Code § 6252(e).

[21] Gov. Code § 6250. "The CPRA provides that 'every person has a right to inspect any public record, except as hereafter provided.' (§ 6253, subd. (a).) Hence, 'all public records are subject to disclosure unless the Legislature has expressly provided to the contrary.' (*Williams, supra,* 5 Cal.4th at p. 346 ….)." (*Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1068.)

[22] Gov. Code § 6255(a) ("The agency shall justify withholding any record by demonstrating that the record in question is exempt under express provisions of this chapter or that on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record.")

[23] Cal. Const., Article 1, § 3(b)(2), *supra*. See e.g., *American Civil Liberties Union of Northern California v. Superior Court* (*ACLU*) (2011) 202 Cal.App.4th 55, 67; and *SCERA*, *supra*, 198 Cal.App.4th at 991-992.

[24] *See e.g.*, *CBS, Inc. v. Block*, *supra*, 42 Cal.3d at 652; *Amgen, Inc. v. Health Care Services*, (2020) 47 Cal.App.5th 716, 732; *ACLU*, *supra*, 202 Cal. App. 4th at 67-68 fn. 3; Gov. Code § 6253(e); *Register Div. of Freedom Newspapers, Inc. v. County of Orange* (1984) 158 Cal.App.3d 893, 905-906; *Black Panthers v. Kehoe* (1974) 42 Cal.App.3d 645, 656; *Re San Diego Gas &* Electric *Company* (*SDG&E*) (1993) 49 Cal.P.U.C.2d 241, 242; and D.05-04-030, at 8. *See* also, the penultimate sentence in Gov. Code § 6254: "This section does not prevent any agency from opening its records concerning the administration of the agency to public inspection, unless disclosure is otherwise prohibited by law."

that even if a record may fall within a CPRA exemption, the agency may still disclose the record if the agency believes no public interest would be served by withholding the record and/or that disclosure is in the public interest.

The CPRA requires the Commission to adopt written guidelines for access to agency records, and requires that such regulations and guidelines be consistent with the CPRA and reflect the intention of the Legislature to make agency records accessible to the public.[25] GO 66-D, effective January 1, 2018, constitutes the Commission's current guidelines for access to its records, and reflects the intention to make Commission records more accessible.[26]

2.2. CPUC General Order 66-D Requirements for Requesting Confidential Treatment of Information

General Order (GO) 66-D sets forth the Commission's procedures for implementing the CPRA. The Network Study covers an 8-year period of the carriers' operations, from January 1, 2010 through December 31, 2017. During most of that period, the Commission's public disclosure and confidentiality guidelines were set forth in GO 66-C, which was effective from 1974 to December 31, 2017. In D.16-08-024, the Commission modified the rules in GO 66-C to require a more robust and detailed showing by utilities claiming confidentiality. This decision governed confidentiality claims until

[25] Gov. Code § 6253.4(b) ("Guidelines and regulations adopted pursuant to this section shall be consistent with all other sections of this chapter and shall reflect the intention of the Legislature to make the records accessible to the public.…").

[26] *See* D.17-09-023, at 11-12, 14; *see* also D.20-03-014, at 22-23 ("Because of the need to promote greater transparency by providing more public access to Commission proceedings and the related documents developed therein, on November 14, 2014, the Commission opened Rulemaking (R.) 14-11-001 [fn. omitted] "to increase public access to records furnished to the Commission by entities we regulate, while ensuring that information truly deserving of confidential status retains that protection." [fn. 56 cites R.14-11-001, at 1.].)

January 1, 2018, when GO 66-D took effect.[27] GO 66-D incorporates the process set forth in D.16-08-024.

GO 66-D governs most of the information the carriers submitted for purposes of this Network Study (*e.g.*, data requests). The service quality reports and underlying raw data and the ARMIS reports were submitted in years 2010-2017 and thus were governed by GO 66-C. Regardless, both general orders required utilities to prove their confidentiality claims.

GO 66-D, § 3, sets forth the requirements for submission of information to the Commission under a claim of confidentiality. GO 66-D, § 3.2, states:

> An information submitter bears the burden of proving the reasons why the Commission shall withhold any information, or any portion thereof, from the public.

To request confidential treatment of information submitted to the Commission, an information submitter must satisfy the following requirements:

a. designate what portions of a document are confidential;
b. state a specific legal basis for the claim (*e.g.* not just "section 583");
c. provide a declaration in support of the claim; and
d. provide a name and email address of a person to contact regarding potential release of information.[28]

GO 66-D further states that if the information submitter cites Gov. Code section 6255(a) (commonly known as the "public interest balancing test") as the legal authority for withholding a document from public release, then the information submitter must demonstrate with granular specificity on the facts of the particular information why the *public* interest served by not disclosing the

---

[27] *See* GO 66-D, § 3.1. Information submitted between September 26, 2016 to December 31, 2017 is governed by D.16-08-024.

[28] *See* GO 66-D, § 3.2.

record clearly outweighs the *public* interest served by disclosure of the record. A *private* economic interest is an inadequate interest to claim in lieu of a *public* interest. Accordingly, information submitters that cite Section 6255(a) as the basis for the Commission to withhold the document and rest the claim of confidentiality solely on a *private* economic interest will not satisfy the requirements of this Section.[29]

In formal proceedings, the ALJ and Assigned Commissioner have discretion with regard to the requirements parties must follow for confidential treatment of information submitted in the proceeding.[30] Nevertheless, parties requesting confidential treatment in a formal proceeding must meet the same burden to demonstrate with particular facts and citation to specific laws why the Commission should not disclose the alleged confidential information.[31]

2.3. Public Utilities Code Section 583

California Public Utilities (Pub. Util.) Code section 583 also governs access to records. Section 583 states in relevant part:

> No information furnished to the commission by a public utility…except those matters specifically required to be open to public inspection by this part, shall be open to public inspection or made public except on order of the commission, or by the commission or a commissioner in the course of a hearing or proceeding.

Section 583 makes clear that even when information is submitted with a claim of confidentiality, the Commission or a Commissioner can release that information in the course of a proceeding.

---

[29] *See* D.17-09-023, at 22, and Appendix A, GO 66-D, § 3.2; D.20-03-014 at 24.

[30] *See* GO 66-D, § 3.3.

[31] *See* CPUC Rules of Practice and Procedure, Rules 11.1 and 11.4.

As noted in numerous Commission decisions, and most recently in D.20-03-014 (*Decision on Data Confidentiality Issues Track 3*) regarding transportation network companies:

> Pub. Util. Code § 583 "neither creates a privilege of nondisclosure for a utility, nor designates any specific types of documents as confidential." (*Re Southern California Edison Company* (1991) 42 CPUC2d 298, 301; *Southern California Edison Company v. Westinghouse Electric Corporation* (1989) 892 F.2d 778, 783 ["On its face, Section 583 does not forbid the disclosure of any information furnished to the CPUC by utilities."]; and Decision 06-06-066, [fn. omitted] as modified by Decision 07-05-032 at 27 [583 does not require the Commission to afford confidential treatment to data that does not satisfy substantive requirements for such treatment created by other statutes and rules.] In fact, Pub. Util. Code § 583 vests the Commission with broad discretion to disclose information that a party deems confidential. (D.99-10-027 [fn. omitted] (1999) CA PUC LEXIS 748 at *2 [Pub. Util. Code § 583 gives the Commission broad discretion to order confidential information provided by a utility be made public.].) As such, a party may not rely on Pub. Util. Code § 583 for the proposition that information required by the Commission to be submitted is confidential.[32]

Accordingly, Section 583 does not provide a substantive basis to withhold information.

2.4. The Commission Favors Open and Transparent Proceedings

Consistent with the California Constitution's and CPRA's requirements that most government records be disclosed to the public absent a specific prohibition or exemption, the Commission has a long history of favoring open and transparent proceedings in the interests of enhancing party participation,

[32] D.20-03-014 at 21-22.

public understanding of utility networks essential to everyday life, and regulatory credibility.

For example, in *In Re Pacific Bell*, D.86-01-026, (1986) 20 CPUC2d 237, the Commission explained the importance of having a process that allows for a "full, open, and expeditious airing of facts," in general rate cases even where the telephone corporation had stamped most of its exhibits as "proprietary."

> Certainly, there are times to be concerned about full public disclosure of proprietary data. Classic examples are customer lists, true trade secrets, and prospective marketing strategies where there is full blown — and not peripheral — competition. To make the assertion stick that there are valid reasons to take unusual procedural steps to keep data out of the public record (*e.g.*, sealed exhibits, clearing the hearing room, or sealed transcripts), there must be a demonstration of imminent and direct harm of major consequence, not a showing that there may be harm or that the harm is speculative and incidental. PacBell must understand that in balancing the public interest of having an open and credible regulatory process against its desires not to have data it deems proprietary disclosed we give far more weight to having a fully open regulatory process.[33]

In *In Re Sierra Pacific Power Company,* D.88-04-016, (1988) 28 CPUC2d 3, the Commission relied on the foregoing policy favoring open access and transparency in its regulatory proceedings to reject unsubstantiated confidentiality claims, stating:

> The Commission intends to continue the policy of openness as enunciated in the Pacific Bell decision and will expect the utility to fully meet its burden of proving that the material is in fact confidential and that the public interest in an open process is outweighed by the need to keep the material confidential. Granting confidentiality to the contract terms requested by Sierra would unduly restrict scrutiny of the

[33] *In Re Pacific Bell*, D.86-01-026, 20 CPUC2d 237, at 252.

> reasonableness of fuel costs and operations. We conclude that Sierra has not adequately demonstrated that any harm to it would occur; therefore, we will deny the request for confidentiality in this order. We believe that Sierra's ratepayers are best served by and protected by open disclosure of contract terms.[34]

These expressions of the Commission's interest in the openness of its proceedings are further reflected in decisions issued by the Commission in R.14-11-001, such as D.16-08-024 and D.17-09-023, and the previously referenced D.20-03-014.

2.5. The Commission Usually Limits Duration of Confidential Treatment of Proprietary Business Information

In general, the Commission does not maintain in perpetuity confidential treatment of information based on an entity's assertion that the information is proprietary business-sensitive information. The Commission usually restricts confidential treatment to two years, implicitly recognizing that the business sensitivity of such information usually diminishes over time.

For example, in D.09-07-019, the Commission rejected AT&T's claim that proprietary cost information (specifically labor rates and task times) that is sensitive, competitive data should remain sealed indefinitely. The Commission

[34] *In Re Sierra Pacific Power Company* (1988), 28 CPUC2d 3, at 11; *see* also D.20-03-014, at 13-14, 30; and D.06-06-066, as modified by D.07-05-032, at 66 ("We intend for parties to treat confidentiality designations with care. They must think about whether they are simply asking for confidentiality as a rubber stamp, or whether evidence truly needs protection. Thus, the requirement that parties show that their data meet the criteria we establish here must have teeth. If there are no consequences of overstating the need for confidentiality, we suspect parties will simply err on the side of asking that too many documents be held under seal.").

allowed the information to remain confidential, but only for a period of two years.[35]

The Network Study covered an 8-year period of the carriers' operations, from 2010 through 2017. The latest utility information summarized or otherwise referenced in the Network Report dates to 2017, a period older than the limited period for which the Commission typically affords confidential treatment to information identified by an information submitter as proprietary financial information.

Thus, as we review AT&T's and Frontier's confidentiality claims, we will consider the Commission's policy of limiting the duration of confidential treatment of business information. We will also consider whether the passage of time has diminished any asserted need for confidential treatment for the information at issue.

3. Overview of Legal Analysis of Carriers' Confidentiality Claims Based on Personal Customer Information, Trade Secret Privileges, the Critical Infrastructure Information Act of 2002, and the CPRA Balancing Test under Gov. Code § 6255(a)

Both AT&T and Frontier rely primarily on laws limiting disclosure of customer information, trade secret privilege assertions, and claims that disclosure is prohibited by the Critical Infrastructure Information Act of 2002 (CII Act). Frontier also contends that a weighing of public interests for and against the disclosure of information under the CPRA balancing test would lead to the conclusion that certain information should be withheld from the public.

---

[35] *See* D.09-07-019 at 80-81 ("The commission usually restricts confidential treatment to two years. … Thus, we will accord confidential treatment to this information for two years**.");** see also *e.g.,* July 28, 2005 Ruling of ALJ Bushey in A.05-01-020, granting motion of Citizens Utilities, dba Frontier, to file under seal certain proprietary business sensitive records for a period of two years from the date of the ruling.

3.1. Personal Customer Information

We have reviewed the Network Report and found that it does not include any personal information relating to individual customers, such as their identities, addresses, telephone numbers, choice of services, or residential or business status. The absence of such information in the actual Network Report makes it unnecessary to discuss personal customer information disclosure issues in detail here.

3.2. Trade Secret Privilege

Evidence (Evid.) Code § 1060 states that the holder of a trade secret has a right to refrain from disclosing a trade secret, and to prevent others from disclosing trade secrets, "if allowance of the privilege would not tend to conceal fraud or otherwise work injustice."[36] "Trade secret" is defined in Civ. Code § 3426.1(d), which falls within the California Uniform Trade Secret Act ("CUTSA"), Civ. Code § 3426, *et seq*., as:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The CUTSA provides a cause of action for "misappropriation" of trade secrets, defined in Civ. Code § 3426.1(b) primarily as the acquisition, use, and disclosure of another's valuable, proprietary, information by improper means.[37]

---

[36] Evid. Code § 1061 states that "trade secret" is defined in Civ. Code § 3426.1(d) and Penal Code § 499(c).

[37] *See e.g., DVD Copy Control Assn., Inc. v. Brunne*r (2003) 31 Cal.4th 864.

Civ. Code § 3426.7 states that: "This title does not affect the disclosure of a record by a state or local agency under the California Public Records Act."

Trade secrets are generally the products of the creativity and hard work of the trade secret holder's efforts to further a business or otherwise reap economic rewards.[38] The idea behind the trade secret privilege is that those who devote time and energy to creating something of value should be protected against the use of such hard won, and economically valuable, information by others who contribute nothing to the creation of the trade secret.[39]

Courts have distinguished between trade secret information versus other secret information:[40]

> It [trade secret] differs from other secret information in a business . . . in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain

---

[38] *See e.g., Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, 1522; *Courtesy Temporary Service, Inc. v. Camacho* (1990) 222 Cal.App.3d 1278, 1287; *American Paper & Packaging Products, Inc. v. Kirgan* (1986) 183 Cal.App.3d 1318, 1326; D.16-01-014; see also, Resolution ALJ-388, *Resolution Denying the Appeals by Uber Technologies, Inc. and Lyft Inc. of the Consumer Protection and Enforcement Division's Confidentiality determination in Advice Letters 1, 2, and 3* (Issued November 16, 2020) at 26, *citing* D.16-01-014 ("While it is true that the word 'information' has a broad meaning, trade secrets usually fall within one of the following two broader classifications: first, technical information (such as plans, designs, patterns, processes and formulas, techniques for manufacturing, negative information, and computer software); and second, business information (such as financial information, cost and pricing, manufacturing information, internal market analysis, customer lists, marketing and advertising plans, and personnel information). The common thread going through these varying types of information is that it is something that the party claiming a trade secret has created, on its own, to further its business interests.")

[39] *See* e.g., *Altavion, Inc. v. Konica Minolta Systems Laboratory, Inc.* (*Altavion*) (2014) 226 Cal.App.4th 26, 42; *DVD Copy Control Assn. v. Brunner*, *supra*, 31 Cal.4th at 880; *San Francisco Arts & Athletics, Inc. v. United States Olympic Com.* (1987) 483 U.S. 522, 536; *Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, 1520.

[40] *See Cal Francisco Investment Corp. v. Vrionis* (1971) 14 Cal.App.3d 318, 322 (citing Restatement, Torts, section 757, comment (b)); *see also*, Resolution ALJ-388, at 7-9.

> employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like. A trade secret is a process or device for continuous use in the operation of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article.

In misappropriation of trade secrets litigation under the CUTSA, to be a trade secret, information must be: 1) information owned by the trade secret asserter, with the trade secret identified with reasonable particularity, sufficient to allow one to distinguish the asserted trade secret from matters of general knowledge;[41] 2) information that is secret – i.e., not generally known to the public, or to other persons who can obtain economic benefit from its disclosure or use;[42] 3) information that has independent economic value from being secret;[43] and 4) information that is the subject of reasonable efforts to maintain its secrecy.[44] "Secrecy is an essential characteristic of information that is protectible

---

[41] Civ. Code § 2019.210; *Altavion*, *supra*, 226 Cal.App.4th at 43; *Diodes, Inc. v. Franzen* (1968) 260 Cal.App.2d 244, 253; *Bunnell v. Motion Picture Ass'n. of America* , 567 F.Supp.2d 1148, 1155 ("A plaintiff must do more than just identify a kind of technology and then invite the court to hunt through the details in search of items meeting the statutory definition [of a trade secret]. [citation omitted]").

[42] Civ. Code § 3426.1(d)(1); *Altavion*, *supra*, 226 Cal.App.4th at 57; *Ruckelshaus v. Monsanto Co.* (1984) 467 U.S. 986, 1002; *DVD Copy Control Assn. v. Brunner*, *supra*, 31 Cal.4th at 881; *AMN Healthcare, Inc. v. Healthcare Services, Inc.* (2018) 28 Cal.App.5th 923, 943.

[43] Civ. Code § 3426.1(d)(2). *See Altavion*, *supra*, 226 Cal.App.4th, at 62 ("Information that is readily ascertainable by a business competitor derives no independent value from not being generally known. [Citation.]" (*Syngenta Crop Protection, Inc. v. Helliker* (2006) 138 Cal.App.4th 1135, 1172 ….)").

[44] *See* e.g., *Vacco Industries, Inc. v. Van Den Berg* (1992) 5 Cal.App.4th at 34 ("Vacco … undertook reasonable efforts to keep it secret. These efforts included (1) extensive internal controls (*e.g.*, visitor logs, sign-out sheets for proprietary documents and a document destruction policy), (2) availability and required use of locked storage cabinets in the engineering department and (3) strict security control measures with respect to documents which necessarily had to be made available to third party vendors or subcontractors. …"); *see*

as a trade secret."[45]

Thus, if a company 1) has invested resources to obtain information it can choose to withhold or make known to others,[46] 2) can identify such information in a manner sufficient to distinguish it from matters of general knowledge,[47] 3) has made reasonable efforts to protect the secrecy of the information (*e.g.*, marking information as a trade secret, educating employees regarding such status, imposing strict controls, limiting physical or electronic internal and external access to the information, requiring nondisclosure agreements),[48] 4) and can demonstrate that the secret information has independent economic value by virtue of being secret (as evidenced, for example, by the willingness of others to pay for the secret information),[49] the company may have a protectible trade secret.

If a claimant asserts that information has independent economic value by virtue of being secret, the claimant should do more than merely assert that the information would be helpful or of use to a competitor recipient in carrying out a specific activity. Such simple assertions are not enough to compel a fact finder to

---

also, *Citizens of Humanity, LLC. v. Costco Wholesale Corp.* (2009) 171 Cal.App.4th 1, 14; *In Re Providian Credit Card Cases,* 96 Cal.App.4th 292, 306-308.

[45] *Altavion*, *supra*, 226 Cal.App.4th at 57. The Supreme Court noted in *Ruckelshaus v. Monsanto Company*, *supra*, 467 U.S. at 1002 ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret. [citation omitted.]").

[46] *Ibid.*

[47] *See* fn. 44, *supra.*

[48] *See* fn. 47, *supra.* Failure to have taken such steps may reasonably be deemed as circumstantial evidence that a trade secret privilege asserter had not previously treated information as a trade secret. *Providian Credit Card Cases, supra,* 96 Cal.App.4th at 308.

[49] *See e.g., Syngenta Crop Protection, supra,* 138 Cal.App.4th at 1172.

conclude the information is sufficiently valuable to provide the claimant with an economic advantage over others.[50]

Information will not fall within the definition of a trade secret if it is readily ascertainable by a competitor or others,[51] if the claimant has not made reasonable efforts to maintain the secrecy of the information[52], or if the claimant fails to substantiate the assertion that the information has independent economic value by virtue of being secret. Nor does information generally available to the public, or to those who can make economic use of it, meet the requirement that trade secret information must be "secret."

The CUTSA provides a cause of action for the misappropriation of trade secrets, as may occur, for example, if someone such as a former employee now in competition with the trade secret holder, or other competitor, obtains the trade secret by improper means, and discloses or uses the trade secret. But not all means of obtaining trade secrets are unlawful; reverse engineering or independent derivation alone are not considered improper means.[53] Similarly, acquiring information from someone who received it from a trade secret holder

---

[50] *See e.g., Yield Dynamics, Inc. v. TEA Systems Corp.* (2007) 154 Cal.App.4th 547, 564-565; *see also id.*, at 565 ("The fact finder is entitled to expect evidence from which it can form some solid sense of *how* useful the information is, e.g., *how much* time, money, or labor it would save, or at least that these savings would be "more than trivial." (Rest.3d., Unfair Competition, § 39.)

[51] *See Altavion*, *supra*, 226 Cal.App.4th at 62.

[52] *See* fn 47, *supra*; see also, *AMN Healthcare, supra,* 28 Cal.App.5th at 943 ("test for a trade secret is whether the matter sought to be protected is information (1) that is valuable because it is unknown to others and (2) that the owner has attempted to keep secret. [Citation.] ... "); *see* also *Ruckelshaus v. Monsanto, supra,* 467 U.S. at 1002 ("if an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.").

[53] Civ. Code § 3426.1(a).

but owed the trade secret holder no duty to keep it secret or limit its use would not be misappropriation.

The CPRA, in Gov. Code § 6254(k), provides an exemption for "Records, the disclosure of which is exempted or prohibited by federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." The Evidence Code includes several privileges that a privilege holder may assert as a basis for refusing to provide evidence and, in certain cases, to prevent others from disclosing information. Such evidentiary privileges include the trade secret privilege (Evid. Code § 1060-1061). If a state agency determines that certain information is subject to one of these privileges, or similar federal or state laws exempting or prohibiting disclosure, it may withhold information from its response to CPRA requests on the ground that such information is exempt from mandatory disclosure, pursuant to Gov. Code § 6254(k). However, while evidentiary privileges such as the trade secret privilege are incorporated into the CPRA as potential bases for an agency to assert the Gov. Code § 6254(k) exemption, an assertion of the trade secret privilege by an entity that submits information to a governmental agency does not guarantee nondisclosure.[54]

A party asserting the trade secret privilege under Evid. Code § 1060 bears the burden of proving that the information it wishes to keep secret meets all elements in the Civ. Code § 3426.1(d) definition of a "trade secret."[55] Evid. Code § 1060 provides that: "If he or his agent (sic) or employee claims the privilege, the owner of a trade secret has a privilege to refuse to disclose the secret, and to

---

[54] *See e.g., Amgen, Inc., supra*, 47 Cal.App.5th at 732.

[55] Cal. Evid. Code § 500: "Except as otherwise provided by law, a party has the burden of proof as to each fact the existence or nonexistence of which is essential to the claim for relief or defense that he is asserting." *See* also, Cal. Evid. Code § 405; *Agricultural Labor Relations Board v. Richard A. Glass Co., Inc.* (*ALRB*) (1985) 175 Cal.App.3d 703.

prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice." Thus, in addition to proving that information falls within the applicable statutory definition of a trade secret, one who wishes to avail of the privilege to refuse to disclose, and to prevent another from disclosing, asserted trade secret information, must meet their burden of proving they meet the Evidence Code § 1060 condition: *i.e.,* that they or their agent or employee "claims the privilege,"[56] and that "allowance of the privilege will not tend to conceal fraud or otherwise work injustice."

After receiving proof sufficient to support a Commission finding that the information is in fact a trade secret; the Commission must then determine whether it believes assertion of the privilege should be allowed, or whether it believes assertion of the privilege would "tend to conceal fraud or otherwise work injustice." If it believes the latter, it is not required to accept the party's Evid. Code § 1060 trade secret privilege claim.

As noted earlier, the Evid. Code § 1060 trade secret privilege is a conditional privilege that can only be asserted where allowance of the privilege would not tend to conceal fraud or otherwise work injustice.[57] Relying largely on *Uribe v. Howie*, *supra*, the Court in *Coalition of University Employees v. The Regents of the University of California* (*CUE*)[58], *supra*, explained that, when an agency seeks to withhold records from the public on the grounds that the records are trade secrets, the court is ultimately required to balance the public's interest

---

[56] Frontier and AT&T do not appear to have explicitly claimed the trade secret privilege when they submitted to the Commission the GO 133-C/D information or ARMIS Report information at issue.

[57] *See e.g., Uribe v. Howie*, (1971) 19 Cal.App.3d 194, 205-207, 210-211.

[58] *Coalition of University Employees v. The Regents of theUniversity of California* (CUE) (Super.Ct. Alameda County, 2003, No. RG03–089302) 2003 WL 22717384.

in disclosure against the public's interest in nondisclosure. The *CUE* Court further explained that *Uribe v. Howie, supra,* construed the "work injustice" language to embody a balancing test analogous to the balancing test required by Gov. Code § 6255(a).[59] Thus, when an agency wants to withhold records on the basis of trade secret privilege assertions, it must first determine whether the records include trade secrets, and then balance public interests for and against disclosure. In *Uribe*, *supra*, *CUE*, and *ALRB*, *supra*, the courts found that the public interest in disclosure outweighed the claimed need for secrecy.

Judicial decisions addressing trade secret privilege claims and the "work injustice" language in Evid. Code § 1060 provides guidance here. While the mere relevance of trade secret information to litigation in which the trade secret privilege is asserted may not necessarily be sufficient to show that the assertion of the privilege would work injustice, some courts have found that:

> the information sought was not just relevant to the general subject matter of the lawsuit and helpful to preparation of the case. Rather, the record in each instance demonstrated prima facie that the information was directly relevant to a material element of the cause of action and further that the moving party would be unfairly disadvantaged in its proof absent the trade secret. Failure to disclose the information would "work an injustice" within the meaning of Evidence Code section 1060 because one side would have evidence-reasonably believed to be essential to a fair resolution of the lawsuit-which was denied the opposing party."[60]

---

[59] *Uribe v. Howie, supra,* 19 Cal.App.3d at 205-0207.

[60] *Bridgestone/Firestone, Inc. v. Superior Court,* (1992) 7 Cal.App.4th 1384, 1392. This "injustice" discussion appears relevant to Commission proceedings as well, although our CPRA-based disclosure determinations are based on an evaluation of the public's interest in disclosure or nondisclosure, and not just the interests of parties to Commission proceedings.

Thus, if an information submitter demonstrates to the Commission's satisfaction that information meets all of the elements necessary for it to fall within the Civ. Code § 3426.1(d) definition of a trade secret, and the Commission determines that the assertion of the trade secret privilege would not tend to conceal fraud or otherwise work injustice, as discussed above, the Commission may withhold such information from responses to CPRA requests, on the basis of Gov. Code § 6254(k), and from responses to discovery, on the basis of Evidence Code privileges.[61]

3.3. The Critical Infrastructure Information Act of 2002

The Critical Infrastructure Information Act ("CII Act") of 2002, codified at 6 U.S.C. § 671 *et seq*., was enacted by Congress to protect key resources and critical infrastructure from computer-based or physical attack. The CII Act protects information related to such resources and infrastructure from disclosure in certain circumstances.

As a threshold matter, we must determine what "critical infrastructure" is. "Critical infrastructure" is defined in the Department of Homeland Security (DHS) regulations, at 6 C.F.R. § 29.2(a) as:

> [S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the

[61] We note that *Amgem*, supra, 47 Cal.App.5th at 734-735, states that:

"It is not clear to us that the trade secret evidentiary privilege is a broad prohibition on disclosure akin to the constitutional right to privacy or the statutory protection for peace officer personnel records. …

Although the legislature expanded the reach of the evidentiary privileges by incorporating them into the CPRA as exemptions, those exemption, like all exemptions under Government Code Section 6254, are not mandatory. "

security, national economic security, national public health or safety, or any combination of those matters.[62]

"Critical infrastructure information" is defined in 6 C.F.R. § 29.2(b) as follows:

> Critical Infrastructure Information, or CII, has the same meaning as established in section 212 of the CII Act of 2002 and means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other information concerning:
>
> > 1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, local, or tribal law, harms interstate commerce of the United States, or threatens public health or safety;
> >
> > (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk-management planning, or risk audit; or
> >
> > (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

[62] 6 CFR § 29.2(a), referring to 42 U.S.C. 5915(c)e.

The DHS website lists 16 critical infrastructure sectors, one of which is the Communications Sector.[63]

The statute, 6 U.S.C. § 671, defines "critical infrastructure information" as information "not customarily in the public domain and related to the security of critical infrastructure or protected systems …."[64]

Thus, for Communications Sector information to be considered "critical infrastructure information" per DHS regulations (6 C.F.R. § 29.2(b)), it must be information provided by telecommunication carriers which is not customarily in the public domain, and which might facilitate an attack, interference, compromise, or incapacitation of a communication utility's network.[65] The fact that information may fall within the broad definition of "critical infrastructure information" does not by itself make such information subject to the CII Act's disclosure limitations.

Pursuant to 6 U.S.C. § 673(a)(1), "critical infrastructure information . . . that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)" is exempt from disclosure under the Freedom of Information Act and is subject to certain restrictions on its disclosure and use.[66] 6 U.S.C. § 673(a)(1)(E),

---

[63] *See* https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[64] *See* also 6 C.F.R. § 29.2(b). Carrier infrastructure information that *is* in the public domain does not fall within the 6 U.S.C. § 671 definition of "critical infrastructure information."

[65] Information readily available on the internet, or through other public sources of information, is "customarily in the public domain."

[66] 6 U.S.C. § 671(2): "The term 'covered federal agency' means the Department of Homeland Security."

extensively cited by AT&T and Frontier, provides that such information, "shall not, if provided to a State or local government or government agency-- (i) be made available pursuant to any State or local law requiring disclosure of information or records; (ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or (iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act. "

However, the disclosure limitations in 6 U.S.C. § 673(a)(1)(E) only apply to protected "critical infrastructure information," as defined in the CII Act and associated regulations, *which is provided by the Department of Homeland Security to a state agency*. Most relevant to this analysis of the carrier's CII Act claims, 6 U.S.C. § 673(c) provides that state and local governments obtaining information *independent* of the CII Act's procedures are not bound by the Act's confidentiality provisions:

> Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local or Federal Government entity, agency or authority . . . *to obtain critical infrastructure information in a manner not covered by subsection (a) of this section*, including any information lawfully and properly disclosed generally or broadly to the public and *to use such information in any manner permitted by law*.[67]

Since the Commission obtained the alleged critical infrastructure information directly from the carriers themselves, rather than from the DHS, 6 U.S.C. § 673(c) explicitly excludes here the 6 U.S.C. § 673(a)(1)(E) disclosure limitations.

[67] 6 U.S.C. § 673(c), emphasis added.

Congress created the Protected Infrastructure Information (PCII) Program under the CII Act to protect private sector infrastructure information that is voluntarily shared with the federal government for purposes of homeland security.[68] 6 C.F.R., part 29, sets forth uniform procedures for the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the DHS.[69]

Under the CII Act, there is a significant difference between "critical infrastructure information" and "protected critical infrastructure information." For "critical infrastructure information," as defined in 6 U.S.C. § 671, to be considered "protected critical infrastructure information," the information must have been voluntarily submitted to the DHS for purposes related to critical infrastructure protection and processed by DHS in accord with its protected critical infrastructure information program procedures. In other words, DHS must have reviewed, approved, and marked the information as falling within its classification of "protected critical infrastructure information."[70] When DHS provides PCII information to a state agency, the state agency's use of such information is limited, and the information would be provided only in association with DHS confidentiality protocols.[71]

---

[68] 6 U.S.C. § 671 *et seq.*

[69] 6 CFR, Part 29, *Procedures for Handling Critical Infrastructure Information; Final Rule,* published in the Federal Register on September 1, 2006.

[70] *See* 6 CFR Part 29, esp. § § 29.5 -29.8.

[71] 6 CFR § 29.3(b).

As noted above, state and local governments obtaining critical infrastructure information independent of the CII Act's 6 U.S.C. § 673 procedures are not bound by the Act's confidentiality provisions.[72]

Here, the Commission acquired the alleged critical infrastructure information directly from the carriers through data requests or reporting requirements, independent of federal laws and procedures.[73] Under these circumstances, this information does not fall under the disclosure restrictions in the CII Act and associated regulations.

Our independent review, however, persuades us of a need to protect certain infrastructure information as a matter of public safety. But, not every piece of information pertaining to infrastructure should be deemed confidential. Whether information should be disclosed may depend on the granularity of the information and the extent to which the information is already public in one form or another. It is in the public interest to reveal information regarding the telecommunications networks to the extent that we can do so without compromising public safety. For our independent review, we will apply the CPRA "balancing test" under Gov. Code § 6255(a), described below.

In asserting its confidentiality claims on infrastructure, Frontier also relies on Gov. Code sections 6254(k) and 6254(e). Government Code section 6254 contains exemptions of particular records under the CPRA. Section 6254(k) exempts the provision of the"[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." Section 6254(e) exempts

---

[72] 6 U.S.C. § 673(c).

[73] Much of this information is publicly available, and thus would not fall within the meaning of "critical infrastructure information" as defined in 6 U.S.C. § 671 or 6 C.F.R. § 292(b).

records relating to "[g]eological data and geophysical data, plant production data, and similar information relating to utility systems development . . . that are obtained in confidence."

While section 6254 states that "this chapter does not *require* the disclosure of the any of the following records,"[74] it does not require that such records be withheld from the public. Thus it *allows*, but does not *mandate,* withholding certain records (unless nondisclosure is required by other laws). Since we have determined that the CII Act is not applicable when the Commission obtains records directly from utilities, section 6254(k) does not apply in this context. Similarly, section 6254(e) allows records to be withheld, but does not bar the disclosure of the records in question. We do not find this exemption applicable to information in the Network Report and do not believe the Commission's assertion of this exemption is in the public interest.

3.4. Gov. Code § 6255(a) – CPRA Public Interest Balancing Test

Gov. Code § 6255(a) is a "catch-all" provision which may be used for determining confidentiality of records not covered by a specific exemption. This provision allows an agency to balance the public interest that would be served by withholding information with the public interest that would be served by the disclosure of the information. If an agency wishes to maintain confidentiality of any records, the agency must find that, on the facts of the particular case, "the public interest served by not disclosing the record *clearly* outweighs the public interest served by disclosure of the record."[75] This is commonly known as "the CPRA balancing test."

---

[74] Gov. Code § 6254, emphasis added.

[75] Gov. Code § 6255(a), emphasis added; *see* also, e.g., *Humane Society of the United States v. Superior Court* (2013), 214 Cal.App.4th 1233.

When submitters of information request confidential treatment based on Gov. Code § 6255(a), they "must identify the public interest and not rely solely on private economic injury."[76] As stated in GO 66-D: "A *private* economic interest is an inadequate interest to claim in lieu of a *public* interest."[77] Further, the California Constitution, the CPRA, and Commission policy all favor disclosure of most government information, and the Commission starts any CPRA "balancing of public interests" analysis with the assumption that the information should be disclosed.

The public has an interest in any information relating to "the conduct of the people's business." Nothing requires the Commission to identify a specific public interest in order to disclose information. Instead, the Commission must justify any withholding of information, based on a specific CPRA exemption, or its determination that, on the facts of the particular case, the public interest served by withholding information clearly outweighs the public interest served by disclosure.[78]

Citizens for a Better Environment v. Department of Food & Agriculture (1985) 171 Cal.App.3d 704, 715, states that: "If the records sought pertain to the conduct of the people's business there is a public interest in disclosure. The weight of that interest is proportionate to the gravity of the governmental tasks sought to be illuminated and the directness with which the disclosure will serve to illuminate."[79]

---

[76] D.17-09-023 at 44.

[77] GO 66-D, § 3.2(b), emphasis in original.

[78] *Costco*, *supra*, 47 Cal.4th at 733.

[79] *See e.g.*, *Connell v. Superior Court* (1997) 56 Cal.App.4th 601, 612.

Balancing interests involves a degree of judgment, and the outcome may vary over time. For example, where information might well "relate to the conduct of the people's business," and thus be subject to the presumption that it should be disclosed, disclosure may at times run counter to other important public interests such as the interest in public safety or personal privacy.[80] The balancing may require an assessment as to how much light disclosure would shed on an agency's actions, or the actions of those it regulates, and as to how much harm might come from disclosure.[81]

The Commission may not delegate to another party the authority to control the disclosure of information that is otherwise subject to disclosure pursuant to this chapter.[82] Thus, when it comes to a decision regarding whether, on the facts of the particular case, the public interest served by nondisclosure clearly outweighs the public interest that would be served by disclosure, it is the Commission, not information submitters, that applies the balancing test under Gov. Code § 6255(a).

Moreover, under Gov. Code § 6257, "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt by law." The fact that parts of a requested

---

[80] *See e.g.*, *CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 652-656, citing *Northern Cal. Police Practices Project v. Craig* (1979) 90 Cal.App.3d 116, 123-124

[81] *Connell v. Superior Court*, *supra*, 56 Cal.App.4th at 613 ("A mere assertion of possible endangerment does not 'clearly outweigh' the public interest in access to these records."), quoting *CBS, Inc. v. Block, supra,* 42 Cal.3d at 652; accord *New York Times, Co. v. Superior Court* (1990) 218 Cal.App.3d 1579, 1585.)

[82] Gov. Code § 6253.3; see also, *e.g.*, *Becerra v. Superior Court* (2020) 44 Cal. App.4th 897.

document may fall within the terms of an exemption does not justify withholding the entire document.[83]

4. Discussion and Analysis of Category 1 Information: General Order 133-C/D Service Quality Reports and Underlying Raw Data

Category 1 information consists of General Order 133 C/D Service Quality Reports and the underlying raw data for "Customer Trouble Reports" and "Out of Service Repair Intervals," which AT&T and Frontier/Verizon submitted from 2010 through 2017 as part of their ongoing service quality reporting requirements. The Network Report includes this information in Chapters 2 (Introduction and Background for This Study), 4 (ILEC Responses to Service Outages), 4A (Service Quality Analysis: AT&T California), and 4F (Service Quality Analysis: Verizon/Frontier).

The Network Report does not include any personal customer information or details. Rather, the Report uses the underlying raw data to rank each carrier's wire centers by comparing reported Customer Trouble Reports and Out-of-Service Repair Intervals for each wire center.

As background, since 1972, the Commission has ordered public utility telephone corporations to provide service that meets minimum service quality standards set forth in the General Order 133 series.[84] General Order 133-C established a minimum set of service quality standards and measures for

---

[83] *CBS, Inc. v. Block*, *supra*, 42 Cal.3d at 652-653.

[84] *See* Pub. Util. Code § 2896 ("The [C]omission shall require telephone corporations to provide customer service to telecommunication customers that includes, but is not limited to,…(c) Reasonable statewide service quality standards, including but not limited to, standards regarding network technical quality, customer service, installation, repair, and billing. …"); *see* also GO 133-D, § 1.1(a).

installation, maintenance, and operator services for local exchange telephone service in California.

On August 29, 2016, in D.16-08-021, the Commission adopted GO 133-D.[85] While GO 133-D maintained the five service quality measurements adopted in GO 133-C, it expanded a number of GO 133-C's provisions, including establishing monetary penalties for violating its five service quality measures.[86]

The five service measures are as follows:

Service Measure	**Type of Service**
Installation Interval	Installation
Installation Commitments	Installation
Customer Trouble Reports	Maintenance
Out of Service Repair Interval	Maintenance
Answer Time	Operator Services

The Network Study analyzed only two of the five service quality measures: Customer Trouble Reports and Out of Service Repair Interval.

The Network Report explained these two measures as follows:

> (1) Customer Trouble Reports (CTR): A maximum of six (6) trouble reports per 100 working lines for reporting units with 3,000 or more working lines, eight (8) reports per 100 working lines for reporting units with 1,001-2,999 working lines, and ten (10) reports per 100 working lines for reporting units with 1,000 or fewer working lines (§3.3(c)).
>
> (2) Out-of-service (OOS) repair interval: Measured by taking the total number of the repair tickets restored within less than 24 hours divided by the total outage report tickets. The

[85] D.16-10-019 corrects minor errors in the original version of GO 133-D.

[86] GO 133-D, § 2.1.

minimum standard is to repair 90% of all out of service trouble reports within 24 hours (§3.4(b), (c)).[87]

Pursuant to GO 133-C/D, telephone corporations are required to report to the Commission their performance along these five measures. Specifically, they must compile this data monthly and report quarterly,[88] using a standardized form developed by Commission staff (known as a "Service Quality Standards Report Card").[89] These quarterly reports are published on the Commission's website, and thus are not confidential.[90]

In addition to submitting the quarterly service quality reports, GO 133-D requires AT&T and Frontier to submit underlying raw data to substantiate the monthly data reported in these Service Quality Standards Report Cards.[91] AT&T and Frontier claim this raw data warrants confidential treatment.

4.1. Carriers' Confidentiality Claims Concerning Service Quality Raw Data

The Category 1 information at issue pertains to the raw trouble report data for every customer reported billing and non-billing related complaint call. Table 2.2 in the Network Report, Chapter 2, at 57, details the "Principal GO 133-C/D Trouble Report Data Elements." Carriers use this raw data to prepare the

---

[87] Network Report, Chapter 1 at 7.

[88] *See* §§ 3.1(e), 3.2(e),3.3(e), 3.4(e), and 3.5(e) in both GO 133-C and GO 133-D.

[89] *See* GO 133-C, Rule 8 ("8. FORM The attached form is a template for reporting GO 133-C Service Quality Standards. The staff may change this form as necessary."; *see* also GO 133-D, Rule 10 ("10. FORM The attached form is a template for reporting GO 133-D Service Quality Standards. The staff may change this form as necessary. Additional information can be found on the Commission's website.") The form can be found at https://www.cpuc.ca.gov/General.aspx?id=1011.

[90] *See* https://www.cpuc.ca.gov/General.aspx?id=1107. The Commission's Communications Division has posts on its webpage all reporting carriers' Quarterly Service Quality Reports (*i.e.*, service quality report cards) from 2010 to present.

[91] *See* §§ 3.3(d) and 3.4(d) in both GO 133-C and GO 133-D.

required quarterly service quality reports. As explained, the Network Report aggregates and summarizes the raw data but does not include specific data concerning individual customer trouble reports or utility responses to such reports. These raw data summaries appear in Chapters 4 ILEC Responses to Service Outages, 4A Service Quality Analysis: AT&T California, and 4F Service Quality Analysis: Verizon/Frontier.

The Network Report states that AT&T submitted approximately 6.1 million individual trouble report records during the January 2010-December 2017 study period, of which roughly 5 million were identified as Out-of-Service ("OOS") conditions of varying lengths. Prior to Frontier's 2016 acquisition, Verizon California had submitted approximately 1.6 million individual OOS reports through December 2015.[92] After Frontier acquired Verizon California in April 2016, the new Frontier California provided the Commission with the last three months of Verizon's out of-service records (approximately 200,000), and through December 2017 has submitted approximately 1.5-million additional records covering its own ownership period.[93]

Importantly, the Network Report aggregates this data for each of the carriers' wire centers in order to rank each wire center's performance with respect to GO 133-C/D's Trouble Reports and Out-of-Service measures. The Network Report provides greater detail than the G.O. 133-D Service Quality Reports in that those quarterly reports do not provide the service quality measurements for each individual wire center. Instead, the Service Quality Reports provide the total combined measurements for all wire centers.

[92] Network Report, Chapter 1 at 9.

[93] Network Report, Chapter 1 at 9-10.

4.1.1. Frontier's Confidentiality Claims

Frontier states that the raw data files "contain granular, monthly data concerning customer service issues and the underlying causes of those issues impacting specific wire centers" and claims this type of information should be protected from disclosure on various grounds. Frontier argues that the raw data "is confidential both because it contains confidential subscriber information and because it is competitively sensitive, which justifies its protection as a trade secret and under the California Public Records Act ("CPRA") balancing test."[94] According to Frontier, the information in the raw data "reflects a 'pattern,' 'compilation,' 'method,' 'technique' and 'process' regarding sensitive outage network information which derives economic and competitive value from not being known to the public and kept from Frontier's competitors, and Frontier consistently maintains this information as confidential."[95]

Frontier further argues that the raw data constitutes "Critical Infrastructure Information," which the Critical Infrastructure Information Act prohibits from disclosure.[96] On that basis, Frontier argues that "[r]elease of this information would also endanger network security, and critical infrastructure protections are incorporated as a ground for protecting information through Government Code Section 6254(k)."[97]

4.1.2. AT&T's Confidentiality Claims

AT&T states that the raw data includes access line numbers by wire center per month, trouble ticket numbers by wire center by month, and reports per

---

[94] Frontier Response, at 2.

[95] *Id*. at 4.

[96] *Id*. at 4-5.

[97] *Id*. at 3.

hundred lines by wire center per month. AT&T further asserts that neither it nor any other reporting carrier publicly releases such information.[98] AT&T claims disclosure would "allow competitors to the change their own business plans by targeting specific geographies in order to convince customers to change service provider. Consequently, such information is a trade secret protected from disclosure based on Gov. Code § 6254(k), Evid. Code § 1060, Civil Code § 3426 *et seq*., and 18 U.S.C. Chapter 90 *et seq*."[99]

AT&T also states that the raw data includes billing telephone numbers and circuit ID, wire center name and wire center number, class of service (business or residential), individual ticket duration, ticket disposition codes showing trouble causes and locations, and zip code, confidential telephone number and class of service information.[100] AT&T argues, "consequently, such information is a trade secret, with the telephone number and class of service information being also protected from public disclosure based on Gov. Code §6254(k); 47 CFR § 64.2001 *et seq*., the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., and Pub. Util. Code §§ 2891 and 2891.1."[101]

Below we address each of the carriers' confidentiality claims collectively.

4.2. The Network Report Aggregates and Summarizes Raw Data, and Does Not Contain Personal Subscriber Information, Individual Trouble Reports, or Utility Responses

As explained above, the Network Report does not include any customer-identifying information, such as customer telephone numbers or customer

[98] AT&T Response at 3.

[99] *Ibid*.

[100] *Id*. at 3-4.

[101] *Ibid*.

telephone numbers linked to services purchased by the customer. Accordingly, the carriers' confidentiality claims based on potential disclosure of customer or subscriber information are moot for purposes of the Report and need not be addressed here.

The Report also does not include any individual customer trouble reports or the utilities' responses to them. Thus, the following information is *not* at issue: customer names, addresses, contact information, service purchased, or individual out-of-service information (e.g., identity or location of specific utility facilities involved in an out of service event or the specific cause of an individual customer complaint out-of-service event or other outage).

The Report does include tables and charts that reflect aggregated and summarized Customer Trouble Reports and Out-of-Service Repair Interval raw data on a wire-center-by-wire-center basis, and on the basis of number of trouble reports per 100-service-lines. The Report provides each carrier's total number of wire centers and utilizes the raw data to rank each wire center.

These types of statistics summarize the classes of information GO 133-D requires carriers to provide for the purpose of informing customers about carrier performance.[102] Providing this information on a wire center by wire center basis promotes a geographically based understanding of carrier service quality and reliability and helps illustrate any differences in the service and reliability available in urban versus rural areas. Disclosure would also offer opportunities for an analysis of possible changes that may be necessary to bridge urban-rural service and reliability gaps in accord with the goals of the Commission and the

[102] GO 133-D, § 2.2.

State, and with statutory requirements that utilities provide quality service on a nondiscriminatory basis.[103]

Disclosure of granular data that has been aggregated and summarized on a monthly basis, as reflected in the Network Report, would be consistent with general Commission policies regarding complaint information disclosure, as discussed below, and with the GO 133-D intent to develop information to inform customers about utility performance. Accordingly, we authorize disclosure of this aggregated data, as discussed herein.

4.3. Service Quality Raw Data, Submitted Pursuant to GO 133-C/D, are not Trade Secrets

4.3.1. Raw data was provided to the Commission to comply with specific and detailed regulatory requirements, rather than created by the utilities to obtain an economic advantage over others

We reject the carriers' arguments claiming that raw Customer Trouble Reports and Out-of-Service Repair Interval data provided by them as required by GO 133-C/D is utility "information, including a formula, pattern, compilation, program, device, method, technique, or process" that would reasonably fall within the scope of a "trade secret" as defined in Civ. Code § 3426.1(d). Rather, the detailed data simply reflects information about utility performance,[104] rather than reflecting the creativity and hard work of the utilities in creating a product.

---

[103] *See e.g.,* Pub. Util. Code § § 451 ("Every public utility shall furnish and maintain such adequate, efficient, just, and reasonable service, instrumentalities, equipment, and facilities, including telephone facilities, …, as are necessary to promote the safety, health, comfort, and convenience of its patrons, employees, and the public…") and 453 ("…(c) No public utility shall establish or maintain any unreasonable difference as to rates, charges, service, facilities, or in any other respect, either as between localities or as between classes of service…."); *see* also D.01-12-021, at 13-15 (finding that ARMIS data showing excessive out of service intervals demonstrated a violation of § 451).

[104] *Ibid*.

Frontier and AT&T confidentiality declarations submitted with the Category 1 information at issue, as required by GO 133-C/D, do not appear to explicitly assert that the submitted information constitute their "trade secrets" or cite specific trade secret laws. Rather, the declarations assert broad-brush generalized bases for the requested confidential treatment, such as the potential for disclosure to adversely affect their competitive positions, competition, or compromise network security. The declarations are devoid of details demonstrating what independent economic value they would obtain from the information not being generally known to the public.

The Commission has rejected "trade secret" claims in other contexts involving reporting of consumer-related data pursuant to Commission order. In D.16-01-014, the Commission found that a transportation company's, Raiser CA, LLC (Uber), compilation of trip data "put together at the behest of the Commission" was not a trade secret:[105]

> ……the type of consumer data compilations that have been accorded trade secret status are ones that contain client names, addresses and phone numbers that have been acquired by lengthy and expensive efforts (See *MAI Sys. Corp. v. Peak Computer, Inc.* (9th Cir. 1993) 991 F.2d 511, 521, *cert. denied*, 510 US 1033l *Courtesy Temp. Serv. v. Camacho* (1990) 222 Cal.App.3d 1278, 1288.) In other words, the party seeking trade secret protection has, on its own initiative, developed some product or process for its own private economic benefit. In contrast, it is the Commission that has ordered the TNCs to respond, in template format, with the trip data by zip code. The compilation is being put together at the behest of the

[105] D.16-01-014, *Modified Presiding Officer's Decision Finding Raiser-CA, LLC, in Contempt, in Violation of Rule 1.1 of the Commission's Rules of Practice and Procedure, and that Raiser-CA, LLC's License to Operate Should be Suspended for Failure to Comply with Commission Decision 13-09-045,Slip. Op.*, at 47-48.

> Commission, rather than by Raiser-CA for some competitive advantage over its competitors.[106]

The Commission rejected the claim that disclosure of the alleged confidential information would provide competitors an economic advantage.[107]

Here, the Commission similarly requires carriers to compile GO 133-D service quality reports that include Trouble Reports and Out-of-Service Repair Interval data, on a detailed reporting unit level (e.g., exchange or wire center[108]), and with information regarding the number of trouble reports per 100-working-lines within each reporting unit. The purpose of this granular level of reporting is to inform the Commission and to provide customers with useful information regarding carrier service.[109] GO 133-D § 1.3 (v) defines "trouble report" as: "Any

---

[106] *Id*. at 47-48.

[107] *Ibid*.

[108] GO 133-D § 1.3 (o) defines Local Exchange as: "A telecommunications system providing service within a specified area within which communications are considered exchange messages except for those messages between toll points per D.96-10-066 " GO 133-D § 1.3 (y) defines Wire Center as: "A facility composed of one or more switches (either soft switch or regular switch) which are located on the same premises and which may or may not utilize common equipment. In the case of a digital switch, all remote processors that are hosted by a central processor are to be included in the central office wire center."

[109] *See* GO 133-D, § 2.2:

> 2.2 Description of Reporting Levels. These levels have been established *to provide customers information on how carriers perform*. Minimum standard reporting levels are established for each of the service measures. Minimum standard reporting levels are applicable to each individual reporting unit.
>
> a. Description. Service affecting, and out of service trouble reports, from customers and users of telephone service relating to dissatisfaction with telephone company services. Reports received will be counted and related to the total working lines within the reporting unit in terms of reports per 100 lines.
>
> b. Measurement. Customer trouble reports received by the utility will be counted monthly and related to the total working lines within a reporting unit. ….
>
> d. Reporting Unit. Exchange or wire center, whichever is smaller. A wire center with fewer than 100 lines should be combined with other central offices within

oral or written notice by a customer or customer's representative to the telephone utility which indicates dissatisfaction with telephone service, telephone qualified equipment, and/or telephone company employees." Trouble reports include out-of-service trouble reports, which would contain the Out-of-Service Repair Interval information.

In addition, the service quality reporting requirements were not intended to develop information for the economic benefit of carriers. The Commission ordered these reports and the underlying raw data to carry out statutory mandates and to inform the public.[110]

The burden is on the information submitter to prove that the submitted information meets all the elements of the trade secret definition in Civ. Code § 3426.1(d) and that the submitter is entitled to assert the conditional Evid. Code § 1060 trade secret privilege. Neither AT&T, nor Frontier have met that burden with the specificity that GO 66-D requires.

4.3.2. Trouble report data consists of customer-submitted complaints and carrier responses to such customer complaints, and is not a trade secret

Contrary to the carriers' claims, raw trouble reports (sometimes referred to as "trouble tickets") are based on information from customers, rather than on the business plans or other efforts carriers engage in for the benefit of their businesses or customers. In other words, trouble reports contain information relayed to the carriers from their customers, which GO 133-D §§ 3.3(d) and 3.4(d) require the utilities to submit. Thus, this type of customer complaint data, which

---

> the same location. A remote switching unit with fewer than 100 lines should also be added to its host switch. URF CLECs that do not have exchanges or wire centers shall report at the smallest reporting unit. All reporting carriers shall submit the raw data included in the report. (Emphasis added.)

[110] *See* Pub. Util. Code § 2896.

was aggregated and summarized in the Network Report, do not constitute the carriers' protectible trade secrets.

Carriers' responses to trouble reports are derivative of, or basically subsets of, information associated with the complaints, rather than wholly distinct carrier-originated information of a type one might consider to fall within the scope of the type of trade secret information described in Civ. Code § 3426.1(d). Information regarding a carrier's response to individual trouble reports would not have been generated by the carrier had the carrier not received the customer complaint in the first instance, and had the Commission not required this type of information to be reported in Commission specified formats.[111] Thus, the underlying, aggregated raw service quality data that is summarized in the Network Report is simply information about the carriers' poor service quality performance, rather than information developed through creativity and hard work falling within the definition of trade secret..

4.3.3. Complaint data, including trouble report data, is not secret

To be a trade secret, information must generally be "secret."[112] Trouble reports are essentially customer complaints. They are similar to informal complaints received by the Commission's Consumer Affairs Branch, which are not inherently confidential. Statistics regarding the number and type of informal complaints against individual telecommunications, energy, and water utilities the Commission receives each month are posted on the consumer information

[111] *See* https://www.cpuc.ca.gov/communications/ link for Service Quality Filings.

[112] *See* fn. 60, *supra*.

portion of the Commission's website. The quarterly service quality reports required by GO 133-D are also posted.[113]

When the Commission receives CPRA records requests seeking information about complaints against specific utilities, either on a state-wide or more location-specific basis, such information is provided, after redaction of personal information concerning complainants (*e.g.*, complainant name, street address [but not city], utility account number, and contact information), where disclosure would constitute an unwarranted invasion of personal privacy.[114] While the Commission does not routinely summarize and post raw GO 133-D trouble report and out-of-service data on a monthly, wire center location-specific basis, this is a matter of choice, rather than because of any specific disclosure prohibitions.

GO 133-D § 6.4 states: "Commission Staff reports. The staff may compile and post the minimum service standards and the performance of each carrier on the Commission's website."[115] GO 133-D implements statutory mandates in Pub.

---

[113] *See* https://www.cpuc.ca.gov/communications/ links for Service Quality Reports.

[114] *See e.g.*, Res. L-441 (authorizing disclosure of incident reports, complaints, and investigation reports relating to contact and/or stray voltage, with appropriate redactions): "records of formal complaint proceedings are available to the public, with the understanding that those who file such complaints are themselves voluntarily making their identities and other personal information public. … Second, we have been making informal complaint records available to the public for many years. If the request for such records is received from the complainant his or herself, or the utility that is the subject of the complaint, we provide the entire file; if the request is from someone ese, we redact the informal complaint's name, address, telephone number, e-mail address, account number and other personal information prior to disclosure. This process … permit[s] us to segregate information subject to a CPRA exemption such as the Cal. Gov. Code § 6254(c) exemption for 'records, the disclosure of which would constitute an unwarranted invasion of personal privacy.'")

[115] While the Commission makes public the service quality reports referenced in GO 133-D, § 6.4, it does currently afford confidential treatment to major outage reports submitted pursuant to § 4.d Major Service Interruption Reports.

Util. Code § 2896(c), which directs the Commission to require telephone corporations to meet "reasonable statewide service quality standards, including but not limited to, standards regarding network technical quality, customer service, installation, repair, and billing." Given that Frontier and AT&T submit to the Commission reports that are based on raw data about each of the service quality standards, including Trouble Reports and Out-of-Service standards, and GO 133-D contemplates that those reports should be made public, we do not see how raw data that was aggregated in the Network Report could be a "secret,"[116] in terms of meeting the elements of a trade secret.

Customer complaint information obtained from a compilation of individual trouble tickets would provide the public with important utility service quality and public safety information. Out-of-service information associated with trouble reports and utility responses to such trouble reports can be helpful in understanding what factors affect network reliability, which affects both general service quality and public safety. The analysis of this information is precisely why the Commission ordered the Network Study.

Accordingly, disclosure of carrier performance based on the *aggregated* monthly data of raw trouble reports by wire center and trouble reports per 100-working-lines, as are contained in the Network Report, would be consistent with both GO 133-D and the Commission's general policies regarding the disclosure of complaint information.

[116] *See e.g.*, *Amgen*, supra, 47 Cal.App.5th at 723, 733-736.

4.3.4. Service quality raw data appearing in the Network Report, aggregated on a monthly basis by wire center, is not a trade secret that has independent economic value by not being generally known

We reject the carriers' arguments that the raw data for Customer Trouble Reports and Out-of-Service Repair Intervals derives the type of economic value associated with a trade secret. To be a trade secret, information must derive "independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use."[117]

Typically, such economic value is derived from the trade secret holder's ability to market a product or service the holder created, and one which is not easily replicated by competitors who have not invested time and resources to develop. Economic value also can mean benefitting from unique customer or client lists developed over time through hard work and relationships, without having others obtain and use those special customer or client lists for competitive purposes.[118] The trade secret holder derives positive value from being able to sell products or services or use painstakingly developed customer lists that they developed solely, and which others cannot access.[119]

While "negative" information may have independent economic value in certain circumstances, such as where a company's research has determined that a

---

[117] Civ. Code § 3426.1(d)(1).

[118] *See e.g., Morlife v. Perry, supra* ("customer list had independent economic value based on its secrecy because it provided a substantial business advantage; "Morlife's customers were not readily ascertainable, but only discoverable with great effort, and the patronage of such customers was *secured through the expenditure of considerable time and money*.")(Emphasis added.)

[119] *Ibid.*

particular formula or approach does not work, the negative information has protectible value because it still derives from the company's efforts.[120]

AT&T and Frontier do not describe any economic value they derive from the raw data not being generally available to the public beyond the value from alleged potential, unnamed, competitors not having access to network descriptions and largely negative service quality information the competitors might use to lure AT&T's customers to switch service providers.[121] This argument is weak.

For one thing, customers and potential competitors can already see how well AT&T and Frontier are performing by looking at their publicly available GO 133-D reports. The carriers' arguments are less an assertion of "independent economic value" related to a carrier-developed trade secret, but rather an expression of concern that disclosure of detailed information required in a Commission-developed report would lead others to compete for customers. No direct connection exists here between information concerning product and service quality, and trade secret status. Indeed, public information concerning product quality, service quality, and price is a common and essential element of many competitive markets.

4.3.5. Title 18 U.S.C. Chapter 90 *et. seq*. does not support trade secret protection for raw data, as aggregated in the Network Report

AT&T cites Title 18 U.S.C. Chapter 90 et seq., as authority for trade secret protection of its raw data. 18 U.S.C. Chapter 90 *et seq*. (18 U.S.C. §§ 1831-1839),

---

[120] *See e.g., Self Directed Placement Corp. v. Control Data Corp*. (1990) 908 F.2d 462; *Genentech, Inc. v. JHL Biotech, Inc*. (2019) (N.D. Cal.) 2019 WL 1045911.

[121] Frontier Response at 4; AT&T Response at 3.

defines certain federal crimes related to economic espionage and the protection of trade secrets in contexts which appear distinct from the instant proceeding. For example, section 1831 relates to "economic espionage" for the benefit of foreign governments, and section 1832(a)(2) prohibits uploading a trade secret, among other things, within the context of "theft of trade secrets." Section 1833 sets forth certain exceptions to these prohibitions, providing that "This chapter does not prohibit or create a private right of action for: "any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; "[122] Thus, the federal prohibition in 18 U.S.C. Chapter 90 does not apply here.

Based on the foregoing analysis, we conclude that the Customer Trouble Reports and Out-of-Service Repair Interval raw data that is presented in the Report in the form of tables and charts summarizing monthly data by wire center, including underlying causes of those issues impacting specific wire centers, wire center ranks, total number of wire centers for each carrier, and any text describing the same, do not constitute protected trade secrets.

4.4. Gov. Code § 6254(e) Does Not Bar Disclosure of Aggregated Raw Trouble Report and Out-of-Service Raw Data

Frontier's reference to Gov. Code § 6254(e) does not provide a compelling basis to withhold disclosure of aggregated raw data concerning trouble reports and associated information. As explained above, Gov. Code § 6254(e) provides agencies with a *discretionary* exemption they may choose to assert if they wish to withhold "[g]eological and geophysical data, plant production data, and similar information relating to utility systems development, or market or crop reports,

[122] 18 U.S.C. §11833(a)(1).

that are obtained in confidence from any person" when responding to a records request.[123] Further, none of this type of information appears in the raw Customer Trouble Reports and Out-of-Service Repair Intervals data analyzed in the Network Exam Report. Therefore, this section is inapposite.[124]

4.5. The Network Report's Aggregation of GO 133 C/D Raw Data Does Not Include Protected Critical Infrastructure Information

We also reject Frontier's claim that Category 1 raw data should be protected as Critical Infrastructure Information. The Network Report contains few references to specific outages and their causes, but none of these contain exact location information of vulnerable facilities, or to any other specific details that could be of more than speculative use to bad actors.[125]

Nor would disclosure of the Report's summaries of Category 1 Customer Trouble Reports and Out-of-Service Repair Interval reports at the wire center or

---

[123] The term "records relating to "utility system development" is too vague to be particularly useful in most records disclosure contexts. Records concerning utility projects subject to review by the Commission and/or other agencies pursuant to environmental protection laws might in theory be considered to be related to utility system development, yet public disclosure of records concerning such projects is essential and required for environmental review. In addition, records relating to existing utility facilities would not usually fall within the scope of records relating to utility system *development*.

[124] The Commission rarely relies on § 6254(e) to withhold information. *See* e.g., Resolution L-597 at 16.

[125] *See e.g.*, *County of Santa Clara v. Superior Court* (2009) 170 Cal.App.4th 1301, 1329: "Security may be a valid factor supporting nondisclosure. … But the "mere assertion of possible endangerment does not 'clearly outweigh' the public interest in access to these public records." (*CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 652, …; accord, *Commission on Peace Officer Standards and Training v. Superior Court, supra,* 42 Cal.4th at 302, …)"; *Connell v. Superior Court* (1997) 56 Cal.App.4th 601, 612-613: "The Controller has presented nothing other than speculation in her supporting declarations that the incidence of counterfeiting will increase if she provides the requested information. This is insufficient."); see also, CPUC Resolution L-459 (2014) (authorizing disclosure of records concerning an attack on a utility substation, with very limited redactions of information that the Commission determined might, if disclosed, pose more than a speculative security risk, and Resolution L-475).

Central Office level raise serious security concerns, since the summaries do not identify any individual utility equipment associated with outages or other types of poor service that might reflect location specific system vulnerabilities.[126] Further, wire center information, including specific locations, is publicly available on various websites.[127]

Moreover, the data at issue is three to ten years old, and therefore any theoretical value of confidential treatment of information showing poor performance in particular portions of the carriers' networks is certainly diminished, if not eliminated.

Since Frontier provided us with the information directly, the 6 U.S.C. § 673(a)(1)(E) restriction simply does not apply, as we discussed in the background section concerning the CII Act;[128] instead, 6 U.S.C. § 673(c) fully

---

[126] *Id*.

[127] *See e.g.*, http://www.thedirectory.org/pref/cosearch.htm; *see* also http://www.thecentraloffice.com/; see also http://www.co-buildings.com/; *see* also https://www.geo-tel.com/central-office-locations/; see also https://www.telcodata.us/search-area-code-exchange-detail; *see* also https://www.sandman.com/cosearch. Such public domain infrastructure information does not fall within the 6 U.S.C. § 671 definition of critical infrastructure information.

[128] *See* Frontier Response, at 6 ("This Critical Infrastructure Information was voluntarily provided to the Commission in expectation of protection from disclosure as provided by 6 U.S.C. § 673(a)(1)(E).") Frontier's reference to its "expectation of protection as provided by 6 U.S.C. § 673(a)(1)(E)" adds no legal weight to its argument, since it is not reasonable for Frontier to assume we share its belief that such information is "critical infrastructure information" or that such information is subject to protection pursuant to § 673(a)(1)(E). We received the information directly from Frontier, and not as information reviewed by the Department of Homeland Security (DHS), officially designated as "protected critical infrastructure information" by DHS, and then provided to the Commission pursuant to DHS nondisclosure protocols. *See* 6 U.S.C. § 673(c); *see* also *Re New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Report and Order (FCC 04-188), at 24 ("The Critical Infrastructure Information Act of 2002…states specifically that "[n]othing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law to obtain critical infrastructure information in a manner not covered by [the 'voluntary submission' subsection]

authorizes our use and disclosure of such independently obtained information. We explained this issue at length in Resolution L-597 (December 17, 2019), which addressed the disclosure of certain fire investigation records, including certain records the utility identified as including critical infrastructure information barred from disclosure by 6 U.S.C. § 673(a)(1)(E).[129] Accordingly, disclosure of the Category 1 raw data in the Report is not prohibited by the CII Act.

4.6. The Carriers' Gov. Code § 6255(a) CPRA Balancing Test Assertions are Unpersuasive

We are not persuaded that the balancing of interests weighs in favor of withholding the Category 1 raw data, as Frontier and AT&T contend. Frontier argues that "public release of this raw data would violate customer privacy rights,… facilitate unfair competition, and pose a security risk," which would "materially harm consumers" and "any public benefit associated with the disclosure of this type of information is far outweighed by the extensive harm that would likely occur from public disclosure through the regulatory process."[130] Frontier also asserts disclosure could "compromise the competitive market," without providing details as to how this might occur.[131]

AT&T does not reference Gov. Code § 6255(a), but similarly asserts that disclosure of raw GO 133-C/D trouble reports data would result in unfair competition because neither AT&T nor its competitors make such information public, and its competitors might use such information to target competition for

---

of this section . . ." In addition, before voluntarily submitted information is entitled to protection, the DHS must first review it and make an affirmative determination as to whether that information does, or does not, qualify as Critical Infrastructure Information ("CIII").")

[129] Resolution L-597 at 14-16.

[130] Frontier Response at 3-4, citing Gov. Code § 6255(a).

[131] Frontier Response at 3.

AT&T's customers.[132] AT&T claims such information is therefore a trade secret, but we dismiss that claim above.

As explained above, the "CPRA balancing test" in Gov. Code § 6255(a) allows state agencies to withhold records in response to a records request, if an agency determines that, on the facts of the particular case, the public interest served by not having the information available to the public clearly outweighs the public interest in disclosure.

In this proceeding, the Commission previously rejected similar claims of harm by AT&T and Verizon when it found that unadjusted out-of-service trouble reports data compiled from carriers' GO 133-C raw data submissions and aggregated on an annual basis should be disclosed.[133] Then, Verizon had filed a statement arguing that "its competitors are not required to provide this type of information, yet those competitors could use the information in marketing against Verizon, which would place Verizon at an unfair business disadvantage vis-à-vis these competitors."[134] AT&T failed to file a statement substantiating its confidentiality claim and thereby waived it.[135] In denying Verizon's confidentiality claim for the raw data, the ALJ wrote:

> Verizon fails to meet the Commission's minimum compliance standard for out-of-service repair intervals by significant margins, and similarly retains a slightly better compliance rate than its largest competitor … Verizon does not explain how a competitor, with access to the adjusted data, would gain a material marketing advantage over Verizon by obtaining access to the

[132] AT&T Response at 3.

[133] *See* R.11-12-001, *Administrative Law Judge's Ruling Denying Request by Verizon California Inc. for Confidential Treatment of Unadjusted Outage Information*, October 6, 2014.

[134] *Id*. at 2-3.

[135] *Id*. at 2.

> unadjusted data that has been aggregated from monthly to annual amounts. These facts substantially undermine Verizon's claim that releasing the unadjusted data would subject it to an "unfair business disadvantage."[136]

Though we are looking at the raw data at a more granular level here, monthly versus annual, we find that AT&T's and Frontier's unfair business advantage and harm claims are as equally unavailing as Verizon's.

We are not persuaded that the public interest served by keeping the information confidential clearly outweighs the public interest that would be served by disclosure as required under the CPRA "balancing test" exemption. Disclosure would provide customers with information about utility performance, in line with the intent of GO 133 to provide the public with a greater understanding of service quality and out-of-service issues at a granular level, and provide information of use to parties to this proceeding and others interested in our network review.

On the other hand, withholding this information would appear primarily to serve only the economic interests of AT&T and Frontier by withholding negative service quality information from those who may seek to compete for the customers of AT&T and Frontier. The public interest in disclosing this information, however, outweighs these unproven economic interests.

The Commission needs this Category 1 aggregated Customer Trouble Reports and Out-of-Service Repair Interval data to ensure telephone corporations "provide customer service to telecommunication customers" that meets "reasonable statewide service quality standards, including, but not limited to, standards regarding technical quality, customer service, installation, and

[136] *Id*. at 3-4.

repair."[137] We must also ensure Californians have safe and reliable telecommunications services.[138]

The Network Study, as detailed in the Network Report, provides us the empirical data we need to determine whether the Commission and the carriers have met statutory responsibilities. Thus, even if disclosure might expose these carriers to greater competition, we do not view such competition as unfair or to be avoided at the cost of informational transparency.

Further, we disagree with assertions that disclosing aggregated, summary customer complaint and out-of-service information at a wire center or Central Office level poses a security threat. The 2010-2017 service quality data in the Report is general in nature.

Finally, we note that the Report does not include individual customer information, and thus does not raise privacy concerns.

In sum, after reviewing the carriers' trade secret, critical infrastructure information, unfair competition/competitive disadvantage, and Gov. Code § 6255(a) balancing test claims, we find no compelling legal authority or factual basis for concluding that the Category 1 information in the Report should not be disclosed. Therefore, we conclude that the non-customer identifying, aggregated raw data related to trouble reports and out-of-service measures discussed herein, including each carrier's number of wire centers and the rank of each wire center, as shown in tables, charts, or text in the Network Report, should be made public. Specifically, we order that Chapters 2, 4, 4A, and 4F in the Network Report be released in their entirety.

---

[137] Pub. Util. Code § 2896.

[138] *See e.g.,* Pub. Util. Code §§ 709, 2896 and 2897.

5. Discussion and Analysis of Category 2 Information: Carriers' Data Request Responses Concerning the Network Study

Category 2 information consists of responses that AT&T and Frontier submitted to ETI and the Commission in response to staff's Network Study-related data requests ("DRs") to the carriers concerning their network infrastructure and company policies and practices. Category 2 information appears in the following Network Report chapters: Chapter 3 (California ILEC Network Overview), Chapter 5 (Infrastructure Policies and Procedures: AT&T), Chapter 6 (Infrastructure Policies and Procedures: Frontier), Chapter 9 (Assessment of Safety, Redundancy and Resiliency of Network(s): AT&T), and Chapter 10 (Assessment of Safety, Redundancy and Resiliency of Network(s): Frontier).

AT&T and Frontier assert that many of the Category 2 DR responses include information that should be accorded confidential treatment because the information is a trade secret, on the basis that disclosure could benefit competitors and result in unfair competition. They also assert the information is critical infrastructure information, which, if disclosed, could be of use to those seeking to harm utility facilities.

As with the carriers' trade secret claims, we will apply the CPRA balancing test to the carriers' critical infrastructure claims because the federal CII Act is not applicable here, where the carriers directly submitted the information at issue to the CPUC. We will include our CPRA balancing test legal analysis in each of the Trade Secrets and Critical Infrastructure Information discussions below.

5.1. Trade Secrets

5.1.1. Frontier DR Responses at Issue

Frontier seeks confidential treatment for several of its Network Study DR responses on the basis that the information contains trade secrets. To support its

trade secret claims, Frontier argues that because competitors are not required to reveal such information, disclosure would foster unfair competition and distort the competitive market. Frontier also asserts that, under the balancing test,[139] the potential harm from disclosure far outweighs any potential public benefits from disclosure. We address each Frontier DR response at issue below.

a. Response to DR 01-F, Question 2, Attachment ("Los Gatos OOS Data for Ntwk Exam Site Visit 01-F with addresses CONFIDENTIAL")

Staff's DR 01-F, Question 2, asked Frontier to provide the following information:

> 2) Maps (by county) of Frontier (Verizon) Communications' operating regions with corresponding names of geographical regions.
>
> a. Regional descriptions should include Division and/or District names (where applicable). The names should be provided as a list with a means of cross referencing to the maps.
>
> b. Include names of wire centers for each district/division

Frontier objects to disclosure of DR 01-F, Question 2, Attachment ("Los Gatos OOS Data for Ntwk Exam Site Visit 01-F with addresses CONFIDENTIAL"), arguing:

> This attachment contains the addresses of specific customers who subscribe to Frontier's services broken down by Central Office, circuit IDs and OOS quarters. For the reasons stated in Section II, in addition to constituting a trade secret and protected confidential information under the CPRA's balancing test, Frontier also has a duty to protect this

[139] *See* Gov. Code § 6255(a).

> confidential subscriber information and CPNI pursuant to state and federal law.…[140]

This argument lacks merit.

As explained above, the Network Report does not include specific customer information and thus no customer information is at issue. In our discussion of the Category 1 service quality raw data, we find that the OOS information in the Network Report does not meet the elements of a trade secret, nor should the information be protected through the Commission's application of the CPRA balancing test. Therefore, the information from DR 01-F, Question 2, Attachment (Los Gatos) that appears in the Network Report should be disclosed.

b. Responses to DR 03-F (Attachments 1-3) and DR 04-F (Attachments 1-2) concerning Frontiers Uniform System of Accounts, Telecommunications Plant in Service accounts

Staff's DR 03-F,[141] Questions 1-7, requested Frontier to provide financial and forecast information from the carriers' 47 CFR Part 32 Uniform System of Accounts ("USOA") Telecommunications Plant in Service ("TPIS") accounts. Staff's DR 04-F, Questions 1-10, asked Frontier to provide information related to the company's policies, practices and procedures regarding infrastructure, facilities and resources. The questions specifically asked about Outside Plant Engineering, Construction & Engineering, Technical Field Services and Central Office departments.

---

[140] Frontier Response at 7.

[141] *Ibid*.

Frontier objects to disclosure of certain attachments provided in response to the questions in DR 03-F and DR 04-F, on the basis that they reveal information about specific accounts that are alleged trade secrets. Frontier provided the following descriptions of the contents of each attachment at issue:

- **DR 03-F, "DR 3 Confidential Attachment 1":** "This attachment contains account-specific information regarding plant addition retirements, and depreciation expenses."[142]
- **DR 03-F, "DR 3 Confidential Attachment 2":** "This attachment contains account-specific information regarding plant addition retirements, and depreciation expenses."[143]
- **DR 03-F, "DR Confidential Attachment 3":** "This attachment contains operating expense charges for specific accounts and associated wire center serving areas."[144]
- **DR 04-F, "DR 4 Attachment 1_Confidential":** "This attachment contains account-specific financial data of construction project investment by exchange."[145]
- **DR 04-F, attachment labeled "DR 4 Attachment 2_Confidential":** "This attachment contains account-specific financial data for maintenance and repair expenses."[146]

There is substantial overlap between the USOA account information provided in these DR attachments and the account information at issue in the

[142] Frontier Response at 7.

[143] *Ibid*.

[144] *Ibid*.

[145] *Ibid*.

[146] *Ibid*.

Category 4 ARMIS Reports. Frontier also raises similar confidentiality assertions for these two sets of account information. Therefore, we will address Frontiers' confidentiality assertions for DR 03-F, Attachments 1-3 and DR 04-F, Attachments 1-2 in our analysis below concerning the confidentiality of Category 4 ARMIS Reports.

c. Response to DR 04-F, "DR 4 Attachment 3_Confidential" (Quality Inspection program)

In response to DR 04-F, Questions 1-10, discussed *supra*, Frontier states that: "This section contains detailed information about Frontier's confidential and proprietary procedures for identifying and repairing problems with outside plant, including personnel information and specific functions and assessments performed."[147]

We find that the Network Report does not provide specific details about Frontier's Quality Inspection Program. Rather, the Report provides a very general discussion on pages 352-357, which largely references Frontier's explanations of the Commission's GO 95 rules regarding the design, construction, maintenance and other safety requirements for electrical and communications utility overhead facilities, similar GO 128 rules regarding underground facilities, and Frontier's protocols for complying with those General Orders.[148] The report consists of several paragraphs briefly describing the classes of employees who inspect or oversee the inspection of Frontier's facilities, with no details regarding individual employees. Similar types of

[147] *Ibid.*

[148] Network Report at 352-357.

information may be found in the records of many safety investigations made public in response to records requests or subpoenas.

Frontier does not explain how such information would fall within the definition of a trade secret, or why the public interest served by withholding such general information from the public would clearly outweigh the public interests served by disclosure. Disclosing this information would provide a better understanding of Frontier's infrastructure inspection and maintenance procedures during an extensive network examination with an emphasis on service quality, network outages, and safety and reliability concerns. Frontier's assertion that the information is "confidential and proprietary" is not an adequate justification under GO 66-D. We find no lawful basis for withholding this information.

d. Response to DR 04-F, Question 10

Staff's DR 04-F, Question 10, requested Frontier to provide "workforce planning and availability forecast – labor resources available for the period of 2018-2020," including forecasted number of employees and contractors (by District)(*e.g.*, engineers, supervisors, managers, support staff, technicians, engineers) assigned to the following projects: "OSP Design and Engineering duties," "Outside Plant Construction projects," "maintenance and repair duties for projects," and "Central Office duties." Frontier argues that its response to this question is confidential, describing its contents as containing "detailed personnel planning and availability forecasts by numbers of employees and contractors for specific departments and/or projects."[149]

[149] Frontier Response at 7.

We have reviewed the Network Report for this type of information and found no reference to detailed personnel planning and forecasts of the numbers of employees and contractors available for specific departments and projects specified in Frontier's Response to DR 04-F, Question 10. Accordingly, there are no confidentiality issues in the Network Report related to Frontier's response to this question.

e. Response to DR 05-F, "DR 5 Attachment 4_Confidential"

Staff's DR 05-F requested that Frontier provide information about its Company policies, practices, and procedures regarding Frontier network safety, redundancy and resiliency of infrastructure, facilities and resource management. This DR, as with DR 04-F, also focused its questions on Outside Plant Engineering, Construction & Engineering, Technical Field Services and Central Office departments. The questions in DR 05-F specifically requested information about:

- Central Office and PSAP (Public Service Answering Point) redundancy;
- Overview of internal practices and procedures for redundancy and resiliency processes and procedures that are followed in emergencies;
- Back-up power standards for Central office and electronic field equipment;
- Internal company standards for allocation of resources and labor in the event of major emergencies (e.g., ability to move field staff between regions in states of emergency, mutual aid agreements with other states, and policy that outlines the standard threshold of outages that triggers resource re-allocation or mutual aid);

- Spreadsheet of all Central Offices/Wire Centers in the former Verizon territory (U-1002-C) that are capable of providing FiOS service to customers (FiOS enabled Cos.

Frontier provided a number of attachments in response to DR 05-F. Frontier argues that Attachment 4 is confidential and describes its contents as follows: "This attachment contains all Central Offices capable of providing FTTP [fiber to the premises] broken down by CLLI[150] and street addresses."[151]

The identities, CLLI codes, and street addresses of Central Offices are readily available to the public, and thus would not fall within the definition of a trade secret.[152] Nor do we see any public interest that would be served by withholding such already public information from the public. Information about the availability of FTTP at specific locations is also readily available, often on the telecommunications carriers' websites, or those of their authorized representatives, devoted to marketing. Presently, one can simply enter a city or address into the appropriate search box in existing platforms on carriers' websites, and find out whether a particular service is available at a location.[153] Publicly available information does not fall within the definition of a trade secret, nor can it form a basis for confidential treatment under GO 66-D, § 3.5 and D.17-09-023, at 27.

[150] "CLLI" stands for Common Language Location Identifier. It provides a standard way of describing locations and significant pieces of hardware at those locations.

[151] Frontier Response at 7.

[152] *See e.g.*, www.co-buildings.com/ca ; https: www.telcodata.us/search-area-code-echange-by-clli; https://sandman.com/cosearch.asp; https://www.stuffsoftware.com/cofindernew.aspx.

[153] *See e.g.*, https://www.buyfrontiernow.com/fios/.

f. Response to DR 06-F, "Automated Regulatory Management Information System (ARMIS) reports listed in the data request"

Staff's DR 06-F requested Frontier provide any missing Annual Report (FCC ARMIS) data for years 2010 through 2017. The USOA Report numbers sought were Form 43-01, 43-02, 43-03, 43-07, and 43-08. Confidentiality assertions regarding ARMIS reports will be addressed below in the section on Category 4 ARMIS Reports.

5.1.2. AT&T DR Responses at Issue

AT&T asserts that its responses to the following data requests are confidential because they contain trade secrets:

- DR 01-A
- DR 02-A and DR 02-A Supplement
- DR 05-A and DR 05-A Supplement
- DR 07-A and DR 07-A Supplement
- DR 08-A and DR 08-A Supplement
- DR 09-A and DR 09-A Supplement

AT&T cites the same legal authority and arguments it used to support trade secret claims regarding Category 1 information. AT&T frequently combines assertions that disclosure of information might be of use to competitors wishing to compete with AT&T, or might be of use to "bad actors" wishing to harm utility facilities, with the conclusion that such information is, therefore, a trade secret. We address those assertions below.

a. Response to "Data Request 1: Field Organization and Wire Center information"

Staff's DR 01-A requested site visits to four AT&T wire centers in Mendocino County, and also listed items expected to be inspected (*e.g.*, main distribution frame wiring, Central office switching equipment and associated rack-mounted equipment, cable vault and feeder cable exit, back-up battery plant, standby generator and fuel tanks, interior equipment, logs, documents, cable vault and associated Central Office infrastructure, and outside plant physical inspections).

AT&T argues that the information provided in response to DR 01-A is confidential on the basis that:

> The responses to Data Request 1 include identification and description of the construction engineering, installation and repair departments at AT&T that support legacy voice service . . . [and] information by wire center on the type of switching, switch capacity, switch in-service dates, and whether or not the wire center is broadband enabled…
>
> The release of this information would be harmful to AT&T by allowing competitors to determine how to geographically organize themselves, and then to target AT&T customers to switch to the competitor's service [by knowing] where AT&T customers are located … and what services are offered by AT&T … Consequently, such information is a trade secret…[citations omitted].[154]

AT&T fails to show how such information falls within the Civ. Code § 3426.1(d) definition of a trade secret. Simply asserting that information is a trade secret does not meet the requirements of GO 66-D and D.17-09-023, which require an explanation as to *how* information meets all elements necessary to

[154] AT&T Response at 4-5.

assert a privilege. AT&T has not shown that this information is in fact secret, that it has independent economic value by virtue of such secrecy, and that AT&T has made efforts reasonable under the circumstances to maintain its secrecy.

The assertion that unnamed competitors do not publicly disclose comparable information is both unsupported by any specific reference, and unpersuasive here. The fact that competitors might use the information to compete for AT&T's current customers also does not support AT&T's trade secret claim.

18 U.S.C. Chapter 90, with its focus on economic espionage for foreign governments and the theft or other misappropriation of trade secrets for the economic benefit of someone other than the trade secret holder, is not applicable to the Network Report. As explained, 18 U.S.C. § 1833 provides in part that: "This chapter does not prohibit or create a private right of action for--(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State."

We note that much of the DR 01-A response information that appears in the Network Report is already publicly available, and therefore it cannot be a trade secret.[155] As AT&T has failed to satisfy the Commission's disclosure

[155] *See e.g.*, *Global Protein Products, Inc. v. Le* (2019) 42 Cal.App.5th 353, 367: "We agree with appellants that publication of a trade secret destroys it. Federal cases that have applied California law have consistently concluded that once a trade secret is publicly disclosed in a patent, the information contained in the trade secret is placed in the public domain and the trade secret is subsequently extinguished. (*Forcier v. Microsoft Corp.* (N.D. Cal. 2000) 123 F.Supp.2d 520, 528; *Stutz Motor Car of America v. Reebok Intern., Ltd.* (C.D. Cal. 1995) 909 F.Supp. 1353, 1359.) Likewise, California courts have also concluded that widespread publication of a purported trade secret extinguishes the trade secret. (*DVD Copy Control. Assn. v. Bunner, supra,* (*DVD Copy Control Assn., Inc. v. Bunner* (2004) 116 Cal.App.4th 241, 251, 10 Cal.Rptr.3d 185 [widespread publication of information over Internet may destroy trade secret].)" *See* also, fn. 61, *supra*.

guidelines in GO 66-D and D.17-09-023[156] concerning DR 01-A information contained in the Network Report, the information will be disclosed.

b. Response to "Data Request 2 and Supplements: Facility Deployment and Customer counts"

Staff's DR 02-A requested AT&T to provide Outside Plant Engineering Information for the Network Exam, including the following information:

- Outside Plant facilities maps by Region or Division that show Wire Center Serving Areas with demarcation of individual Distribution Areas (within the wire center serving area) that include a breakdown of installed plant (i.e., areas with service provided solely by copper plant, Digital Loop Carrier systems, areas with Fiber-in-the Loop systems)

- Spreadsheet by Wire Center name and CLLI Code showing the following information: (a) Description of the principal geographic characteristics of the area being served (urban, suburban or rural), (b) Primary customer base, i.e., residential or commercial, (c) Physical properties of the area, flat, mountainous, rivers, lakes, wetlands, (d) List of all census tracts served by the Central Office building, (e) Area (in square miles) of area served by the Central Office

Staff sent AT&T two supplemental data requests to DR 02-A because AT&T's provided incomplete responses to the original DR.

AT&T states that the responses to DR 2 and Supplemental DRs include: (1) A map of the state of California depicting where AT&T has deployed the following technologies: Fiber to the Premises (FTTP), Fiber to the Node (FTTN), Remote Terminal Digital Subscriber Line (RT-DSL), Central Office Digital

[156] D.17-09-023 at 27; GO 66-D § 3.5.

Subscriber Line at speeds greater than 14.7 Mbps (CO-DS › 14.7), and Central Office Digital Subscriber Line at speeds less than 14.7 Mbps (CO-DSL ‹ 14.7); and the location of AT&T's Serving Area Interfaces and Remote Terminals; (2) Access line counts for POTS service and subscribership counts for VoIP service, broken down by wire center and then further by Residential versus Business.[157]

AT&T asserts the above information contains trade secrets, stating:

> Mapping that shows the statewide locations of AT&T Service Area Interfaces ("SAIs") and Remote Terminals is critical infrastructure information. The release of this mapping information would be harmful in that it could provide a comprehensive roadmap for sabotage of AT&T facilities. Consequently, such information is a trade secret protected from disclosure based on California Government Code § 6254(k). Cal. Pub. Util. Comm'n General Order 133-D, 18 U.S.C. § 1905 ….[158]

AT&T further cites the authorities it routinely references relating to its critical infrastructure assertions, which we address separately below.

GO 66-D states that "[i]f the information submitter cites Government Code Section 6254(k) (which allows information to be withheld when disclosure of it is prohibited by federal or state law), it must also cite the applicable statutory provision and explain why the specific statutory provision applies to the particular information."[159] AT&T claims the information is critical infrastructure information, and is thus a trade secret protected from disclosure by Gov. Code § 6254(k), G.O. 133-D, and 18 U.S.C. § 1905, but fails to explain how the

[157] AT&T Response at 5-6.

[158] AT&T Response at 6.

[159] G.O. 66-D, § 3.2(b).

information falls within the Civ. Code § 3426.1(d) definition of a trade secret, when most of this information is publicly available.[160]

Infrastructure information that is in the public domain does not fall within the 6 U.S.C. § 671 definition of "critical infrastructure information," and, in any event, status as critical infrastructure information has no bearing on whether information is a protectible trade secret.

Further, as referenced elsewhere in this decision, requests for confidential treatment based on assertions that information a utility submits directly to the Commission is subject to nondisclosure on the basis of 6 U.S.C. § 673(a)(1)(E) are flawed, as acknowledged in *Re New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-035, Report and Order (FCC 04-188, at 24). GO 133-D provides no support for the confidential treatment of any information other than Major Service Interruption (MSI) outage reports required to be filed with the FCC and the Commission (GO 133-D § 4.d). The MSI reports are not at issue in the Network Report. Moreover, 18 U.S.C. § 1905 imposes certain disclosure restrictions on federal employees, not state agencies, and is thus not relevant here.

AT&T asserts that "access line and VoIP subscribership broken down by wire center and further by Residence and Business service is competitively sensitive information to AT&T," and that competitors could use this information to tailor their offers in order to "target AT&T customers to switch their service provider. AT&T's competitors do not publicly release similar information. Consequently, such information is a trade secret…. "[161]

---

[160] *See e.g.,* footnote 163, *supra*; *see* also, California Interactive Broadband Map on the Commission's website.

[161] AT&T Response at 6-7.

The fact that a competitor might use the information to compete with AT&T does not by itself make the information a trade secret. AT&T's mere assertions that neither AT&T nor its competitors release such information, and that AT&T took steps to keep the information secret fail to satisfy its burden of proving the information in question constitute trade secrets. In any event, while the Network Report includes tables showing certain average access line number information on a wire center basis in summarizing service quality data, it does not include either wire center data broken down by residential vs. business service, or data reflecting VoIP service.

c. Response to "Data Request 5 and Supplements: Central Offices and Public Safety Answering Points (PSAP)"

As with Frontier, staff's DR 05-A and the supplemental data requests to AT&T requested information about AT&T network safety, redundancy and resiliency. AT&T states that the response to DR 05-A and Supplements include: (1) Statewide AT&T Central Office and Public Safety Answering Point (PSAP) Information;[162] (2) Central Office Backup Power Fuel Capacity; (3) AT&T Methods and Procedures entitled "Disaster First Strike Team Job Aid and "Detail Engineering Requirements - Section 12 Power Systems"; and (4) Graphical Depiction of 911 Call Routing.[163]

In addition to asserting that the information contains protected critical infrastructure information, and thus is a trade secret, AT&T essentially repeats its

[162] Including identification of AT&T Central Offices which play a role in serving PSAPS, and the PSAPS associated with each. switch type and model broken down by central office, the type of traffic handled by each Central Office playing a role in serving PSAPs (originating vs. overflow 911), and signaling type.

[163] AT&T Response at 7-9.

confidentiality claims concerning DR 02-A. AT&T claims that disclosing the information "would allow competitors to target their marketing and competitive strategies," and that AT&T's competitors do not publicly release comparable information, the information is a trade secret.[164] As explained, the fact that a competitor might use the information to compete with AT&T does not by itself make it a trade secret. Therefore, AT&T fails to substantiate its trade secret claims for DR 05-A and Supplemental information that appears in the Network Report, which will now be disclosed.

d. Response to "Data Request 7, 8, and 9 and Supplements: Detailed Accounting Data"

Staff DR 07-A requested missing data from DR 03-A[165] and clarifying or corrected information for discrepancies in AT&T's responses to other data requests regarding the number of Central Offices in AT&T's operating areas.

Staff DR 08-A requested additional (and clarification of previously provided) financial information. This supplemental DR asked for additional information concerning USOA accounts and the number of homes passed in each of the Distribution Area boundaries, aggregated for each Distribution Area Technology for each wire center.

Staff DR 09-A requested AT&T to answer questions related to discrepancies in responses to previous DRs and additional requested information in supplemental DRs, including numbers for Gross Plant Addition provided in

---

[164] AT&T Response at 7-8.

[165] The missing data from AT&T's response to DR 03-A related to spreadsheets AT&T provided in three excel spreadsheets: "02-Corrected Attachment 1_DR 03A_Gross Plant Additions.xlsx," "03-Corrected Attachment 2_DR 03-A_Property Retired.xlsx," "04-Corrected Attachment 4_DR 03-A_Operating Expense Charge.xlsx."

AT&T's supplemental response to DR 03-A and discrepancies in amounts reported in AT&T California Forms 43-02 (as filed with the CPUC) and amounts reported in the AT&T's DR responses.

AT&T states that, "in response to this series of data requests, AT&T provided detailed accounting data which showed AT&Ts investments and expenses by specific accounts. As described below, this data is confidential."[166] AT&T then explains that it considers such information a trade secret, citing the authority it has referenced regarding earlier trade secret assertions.[167]

AT&T asserts that Central Office transmission account information, and cable and wire account information, is also critical infrastructure information, subject to disclosure limitations in 6 U.S.C. § 673(a)(1)(E) and other previously referenced authority.[168]

We address trade secret assertions regarding this accounting data in the discussion of Category 4 ARMIS Report data. We address AT&T's critical infrastructure assertions in Section 5.2 below.

5.1.3. CPRA Balancing Test Applied to the Carriers' Competitive Harm Claims

Frontier claims that none of the Category 2 DR responses at issue should be disclosed under the CPRA's balancing test on competitive harm and public safety grounds. As to competition, Frontier argues: (1) Frontier's competitors could use the Category 2 information to gauge the financial condition, network capabilities, investments, operational decisions, and personnel needs of Frontier and to target their operations to compete with Frontier; (2) Frontier does not

[166] AT&T Response at 10 -22.

[167] AT&T Response at 10-24.

[168] *Ibid*.

have access to similar information regarding its competitors; (3) disclosure disparities would create an uneven playing field, harm a competitive market, and harm consumers by distorting market outcomes; and (4) disclosure would be an abuse of the regulatory process to obtain confidential documents.[169] Concerning public safety, Frontier claims disclosure would compromise network security and create risks to public safety.[170]

We disagree with Frontier's competitive harm assertions. Under the CPRA balancing test, information may be withheld if an agency determines that, on the facts of the particular case, the public interest in withholding information clearly outweighs the public interest in disclosing information. D.17-09-023, which adopted GO 66-D, states "but as noted in Section 3.2 [of GO 66-D] the assertion must identify the public interest and not rely solely on private economic injury."[171] "A *private* economic interest is an inadequate interest to claim in lieu of a *public* interest."[172] Information submitters citing the CPRA balancing test (Section 6255(a)) and resting the claim of confidentiality solely on a *private* economic interest will not satisfy the requirements of this section.[173] Frontier's competitive harm claims are primarily tied to protecting its private economic interests, although it also asserts disclosure would somehow harm competitive markets.

The current level of competition has been unable to incentivize Frontier and AT&T sufficiently to meet our GO 133 service quality objectives, despite our

---

[169] Frontier Response at 8-9.

[170] *Id*. at 6.

[171] D.17-09-023 at 44.

[172] GO 66-D, § 3.2(b), emphasis in original.

[173] *Ibid*.

belief that the competitive marketplace should have such an effect. We are not persuaded by Frontier's assertion that it cannot access similar information about its competitors, since the websites that provide detailed information regarding the facilities of Frontier and AT&T provide similar information about other telecommunications carriers as well. [174]

Even if our disclosure of information in the Network Report results in competition for AT&T's and Frontier's customers, such an outcome would not be the result of unfair competition or an abuse of the regulatory process, nor would it harm consumers, as Frontier claims.[175] To the contrary, we would be acting at odds with our regulatory responsibilities to ensure consumers have access to high quality and reliable telecommunications services if we failed to be open and transparent about this Category 2 information, which is germane to the network examination we ordered in an effort to help us understand and improve the networks and operations of AT&T and Frontier.[176]

---

[174] *See e.g.*, https://www.stuffsoftware.com/cofindernew.aspx; *see* also, fn 128.

[175] Frontier Response at 9. Frontier does not identify any specific competitors for its legacy wireline service, a focus of the Network Study. Cf., D.20-03-014. C.F. D.20-03-014, at 16: "Uber and Lyft refer to competitors in opaque terms, thus failing to substantiate that their claims of an unfair competitive disadvantage have any factual validity." Uber claimed unnamed competitors could use disclosed information to "target potential business opportunities that negatively impact Uber" and Lyft asserted that its "trip data is extremely valuable to Lyft's competitors. …The release "would allow a competitor to tailor its operations more effectively by taking the data that Lyft has generated.[.]" *Id.*, fn. 33.

[176] And, as we often discussed elsewhere, much of the Category 2 information Frontier asks us to keep from the public is already public, thus falling outside both the definition of a trade secret, and the scope of information that could be protected under the process set forth in GO 66-D, § 3.2(b).

5.2. Critical Infrastructure Claims for Information Other than G.O. 133-D Service Quality Data

In this section we address the carriers' confidentiality claims regarding information obtained in the Network Study-related data requests that relate to the physical infrastructure of the carriers' networks. Both Frontier and AT&T request confidential treatment of information provided to CD and ETI on the basis that they concern "critical infrastructure information" precluded from disclosure by 6 U.S.C. § 673(a)(1)(E).

As explained *supra*, because the CII Act does not apply to the information the Commission obtained in the DR responses, such information does not meet the definition of "critical infrastructure information" that is restricted from disclosure by 6 U.S.C. § 673(a)(1)(E) or Gov. Code § 6254 (e).

We will apply the CPRA balancing test to determine whether disclosure of certain infrastructure information is in the public interest, and to explore the carriers' specific security concerns. We share the desire to refrain from disclosing information that could present a safety risk to carriers' facilities and the public. We have in the past withheld from the public narrow and specific information that could be of more than vague or speculative benefit to those seeking to harm utilities and the public.[177]

As explained further below, upon careful consideration of the carriers' network security and public safety concerns, we find that a limited subpart of Category 2 infrastructure information obtained from the Network Study-related DRs warrant confidential treatment under Gov. Code § 6255(a), Evid. Code § 1040(b)(2), and Gov. Code § 6254(k). We find that, on the facts of this particular

[177] *See* Resolution L-459 (2014) (responding to a records request for information regarding an attack on an electric utility substation); and Resolution L-475).

case, the public interest that would be served by withholding a very limited amount of information that might, if disclosed, be of potential use to those wishing to harm utility facilities, clearly outweigh the public interest that would be served by full public disclosure of such information at this point. If a change in circumstances arise that require us to reconsider disclosure of such information, we may revisit these determinations.[178] We address the carriers' critical infrastructure claims below.

5.2.1. Frontier DR Responses at Issue

Frontier requests confidential treatment of certain attachments supporting its responses to DRs 01-F, 02-F, and 05-F, "which relate to security, capabilities, characteristics and precise location of Critical Infrastructure Information."[179] Frontier asserts that the information in the attachments is "critical to maintaining the proper functioning and security of Frontier's network, and includes details concerning Frontier's emergency and 911 capabilities.[180] On these grounds, Frontier contends that the public disclosure of this information would compromise network security and public safety.[181]

---

[178] This approach is similar to the one we took in D.17-06-015, *Order Instituting Rulemaking to Adopt Rules Governing Commission Regulated Natural Gas Pipe Lines and Facilities to Reduce Natural Gas Leakage Consistent with Senate Bill 1371*, at 34-35 ("The utilities have argued that making the precise location of underground gas infrastructure leaks known in this proceeding could create a potential safety risk without a corresponding public benefit. In other proceedings, we have not viewed GIS locational data as presenting a heightened security risk for utility infrastructure. However, in this proceeding, GIS level data is not required for the CPUC to fulfill statutory obligations, as more general census tract or zip code locational information is sufficient. Although it is unclear the precise degree of risk that would come from releasing the GIS locational data, the lack of a corresponding benefit weighs in favor of protecting this information at this time.").

[179] Frontier Response at. 5.

[180] *Id*. at 6.

[181] *Ibid*.

In addition to its CII assertions, Frontier claims the information should also be withheld on the basis of being trade secret information that qualifies for confidential treatment under the CPRA balancing test.[182]

a. Response to DR 01-F, Question 1, Map Attachments ("Network Site Visit 01-F Los Gatos Maps Confidential")

Frontier states that the attachment ("Network Site Visit 01-F Los Gatos Maps Confidential") provided in response to DR 01-F, Question 1, contains detailed maps which identify locations of critical infrastructure facilities of specific Central Offices and feeder/distribution routes broken down by copper/no services, fiber to the premises (FTTP), digital loop carrier (DLC), and cross connect.[183]

The maps provided in the attachments at issue appear in the Network Report at 582-583. These maps contain information that public utilities typically do not make public.[184] The detail in the maps exposes infrastructure information that might make it easier for the carriers' networks to be attacked and thus pose a risk to public safety. Therefore, we agree with Frontier that these maps should not be disclosed at this time.

b. Response to DR 01-F, Question 3 (Background Information for Network Exam), Attachment ("DR 01-F #3 Confidential")

Staff DR 01-F, Question 3, requested Frontier to provide Central Office Data, including: (a) CLLI Code, (b) Wire Center Number (if applicable),

---

[182] *Ibid*.

[183] Frontier Response at 5.

[184] We note, however, that similar information may well be available to the public through other sources. See e.g., fn. 194, *infra*.

(c) Central office name, (d) Street Address, I City/Town, (f) Zip code, (g) Type of existing Central Office switches, (h) Capacity of Central Office switch, (i) Date in service, and (j) Broadband enabled (yes or no?). Frontier states that "[t]his attachment contains highly granular data concerning the critical infrastructure of Central Offices, including Common Language Identification (CLLI) codes, wire center number, street addresses, types of existing switches, capacities of those switches, dates in service and whether they are broadband enabled."[185]

In the Network Report, some of this data is used in a narrative that discusses Frontier's switches in aggregate numbers. (Network Report, at 79.) In addition, some tables show switch type, installation date ranges, and number of switches, and the total capacity of each switch. Finally, a table for the Los Gatos wire center, derived from a physical site visit, shows the rank of the wire centers in terms of outage duration, the number of lines, whether they are broadband, population of the area, and the area size in square miles. (Network Report, at 80, Table 2.3 and at 564, Table 12.7.) This information is publicly available in one form or another.[186] Therefore, the Network Report's general discussion of information obtained from this attachment should be disclosed.

c. Response to DR 02-F, Question 1, Attachment ("CPUC Network Audit Data Request 2 Attachment A")

Staff DR 02-F, Question 1, requested Frontier to provide Frontier California company Outside Plant facilities maps by Region or Division that show Wire

[185] Frontier Response at 5-6.

[186] *See e.g.*, https://www.telcodata.us/search-area-code-echange-by-clli; https://sandman.com/cosearch.asp [CLLI code addresses, area code, exchanges and type of switch(es) at each Central Office]; www.co-buildings.com/ca.

Center Serving Areas with demarcation of individual Distribution Areas (within the wire center serving area) that include a breakdown of installed plant.

Frontier states that the Attachment A provided in response to the question contains granular outside plant facility maps showing wire center service areas and Central Office switches broken down by areas served solely by copper, FTTP, DLC/remote, and cross connect.[187] The information Frontier provided in response to this data request includes:

- Total number of wire centers
- Total population where FiOS-capable FTTP Plant has been deployed by Frontier indicated by the total population for each of the following three categories: (1) No Broadband, (2) Non-FTTP Broadband/DSL, and (3) FTTP/FiOS.
- Geographic operating areas and number of wire center per area with map.
- Data on service outages and population density.
- Types of broadband services and population for each of Frontier's Central Offices.
- Maps with details of Long Beach wire center.

Some of this information formed a basis for a narrative portion of the Network Report (at 60). In addition, data was used to compile charts showing the aggregate population at locations where FiOS-capable FTTP plant has been deployed (at 85, Table 3.6); as background for charts showing the drop off in demand in relation to related out-of-service conditions (at 294-299, Figures 4F.26 to 4F.33); the types of broadband at each wire center (at 87-92, Table 3.7); and a table and map of Frontier California's operating areas (at 74-75, Table 3.3 and

[187] Frontier Response at 6.

Figure 3.5). As discussed, this information may be found publicly and therefore should be disclosed.

On the other hand, the maps of each Long Beach wire center should not be disclosed at this time because of public safety concerns. (Network Report, at 93.) This information is detailed and might pose a potential safety risk because it shows the details of specific wire centers.

d. Response to DR 02-F, Question 2, Attachment ("CPUC Network Audit Data Request 2 Attachment B") and Attachment ("Update to DR 2 Q 2 Confidential")

Staff DR 02-F, Question 2, requested Frontier to provide a spreadsheet by wire center name and CLLI Code showing: (a) urban, suburban or rural, (b) residential or commercial, (c) the area's physical properties (*e.g.*, flat, mountainous, rivers, lakes, wetlands), (d) list of all census tracts served by the Central Office building, (e) area (in square miles) served by the Central Office.

Frontier states that "[t]hese attachments contain granular information by wire center and CLLI showing physical and geographic characteristics of each wire center, primary customer base, and urban and non-urban areas by square miles."[188] This type of information is not critical infrastructure information.

Census tract and population data included in the attachment was used as background for a portion of the narrative (Network Report, at 60) and for charts showing the relation of service outages to population (at 294-299, Figures 4F.26 to 4F.33). Much of this type of information in the Network Report came from public sources rather than from the carriers. To the extent these sections of the Report may be based on information not previously made public, the discussion

[188] Frontier Response at 6.

in the Report does not disclose raw data provided by the carriers. Therefore, the Network Report's general discussion of any information obtained from this attachment should be disclosed.

e. Response to DR 05-F, Attachment ("DR 5 Attachment 1 Confidential")

Frontier states that DR 05-F, Attachment 1, contains CLLI codes for each Central Office with physical and/or diverse connections to the Public Switched Telephone Network, which could be used to identify the specific location and function of critical infrastructure.[189] Frontier asserts that those wishing to harm utility networks and the public could use the diversity information associated with particular Central Offices to target those more vulnerable because they lack diversity.

This attachment includes CLLI codes for Central Offices, detailed network maps, and data on whether connections are diverse or non-diverse. (Network Report, at 496-502, Tables 10.1 and 10.2; at 492, 494, 508, Figures 10.2, 10.4, and 10.6.) While the identities, locations, and CLLI numbers of Central Offices are readily available to the public, Tables 10.1 and 10.2 list all the Central Offices according to whether they are diverse or non-diverse. Figures 10.2, 10.4, and 10.6 are detailed maps which contain information that is not normally made public by carriers.

"Diversity" generally refers to telecommunications routing between two points over more than one geographic or physical path. There are different levels of route diversity. Diversity may refer to routes where there are no common line connection points along the way, except potentially at end points,

[189] Frontier Response at 6.

or some other level of diversity. Diversity is important to resiliency and reliability of a telecommunications network because where there are redundant routes there is less chance that damage to one route prevents calls from going through.[190] On the other hand, if a routing system is non-diverse, there is only one route from point A to point B. It is arguable that information regarding non-diverse routes could be used by someone to target the most vulnerable parts of the telecommunications network.

Since diversity is an important factor supporting network safety and reliability, we believe it is important for the public to understand the extent to which Central Office connections are diverse or non-diverse.[191] However, we do not believe this requires full disclosure of the location of non-diverse routes by specific Central Offices. As stated above, it is possible that such information could be used by bad actors to target the most vulnerable facilities, thus posing a security and safety risk. Thus, the public interest served by withholding some of this data clearly outweighs the public interest that would be served by disclosure.

Table 10.1 only lists the Central Offices that have diverse connections. We do not think that disclosure of this information poses a risk to public safety. Since all of the Central Offices listed have diverse connections, they do not reveal

---

[190] The FCC recognizes the importance of route diversity and adequate backup power. FCC regulations in 47 C.F.R. § 9.19 imposes specific backup power requirements for Central Offices serving Public Safety Answering Points (PSAPs) and require carriers providing 911 service to submit annual certifications regarding compliance with backup power requirements and network diversity auditing requirements, and provide that the fact of filing or non-filing of such certifications, and certain information in such certifications, is public information. 47 C.F.R. § 9.20 requires providers of covered services to offer subscribers various backup power solutions and related information.

[191] *See e.g.*, 47 C.F.R. Subpart H, §§ 9.19 – 9.20, FCC regulations regarding resiliency, redundancy, and reliability of 911 communications, and backup power obligations.

any particular vulnerability. Disclosure of Table 10.1 will, however, allow parties and the public to explore whether Central Offices with physical and/or logical diverse connections are located primarily in urban areas, primarily in rural areas, or in a variety of urban and rural areas. Such information is potentially relevant to an assessment of the degree to which Frontier offers the same level of resiliency throughout its service territories, or whether Frontier may be favoring some locations over others.

Table 10.2 lists those Central Offices with nondiverse connections. Accordingly, the Commission will redact the Central Office identity information from Table 10.2 in the Report showing the location of non-diverse connections (column 2 labeled "Central Office" and column 3 labeled "CLLI.")[192] As we have stated previously, if circumstances change, it may become appropriate to revisit this determination.

Would the disclosure of the identities of Frontier Central Offices with diverse connection, and the redaction of the identities of Central Offices without diverse connections enable potential bad actors to identify Central Offices without diverse connections by subtracting the Central Offices with diverse connections from an overall list of Central Offices in a manner that would result in a more than speculative likelihood of harm to Frontier's network and the public? We think not. We assume that Frontier is continuing to strive to improve the diversity of its Central Offices, and thus the resiliency and reliability of its overall network, in response both to its own desire to create a more robust and reliable network capable of responding effectively in the face of increased wildfire risks and other concerns, and in response to the FCC's encouragement of

[192] *See* fn 167.

increased circuit reliability and back-up power capabilities, and that the 2017 snapshot of Frontier's Central Office diversity may reflect a historical situation rather than more recent reality. We believe the above-expressed value of disclosing Table 10.1 in an unredacted form outweighs what we perceive to be minimal risks from disclosure.

We will redact the detailed maps (Figures 10.2, 10.4, and 10.6) because we find that disclosing them presents a risk to public safety.

f. Response to DR 05-F, Attachment ("DR 5 Attachment 2 Confidential")

Frontier states that this attachment contains a list of Central Offices that host specific Public Safety Answering Points (PSAPs) and identifies whether each is diverse.[193] (Report, at 502-505, Table 10.3.)

PSAPs are integral to dispatching first responders in the event of an emergency. The identity and basic location of PSAPs is publicly available on the FCC's website. However, information regarding PSAP connection diversity is not readily available. And, as with Central Office connections, disclosure of the location of PSAPs having nondiverse connections could be used by a bad actor to find where the network is most vulnerable. Thus, we will follow the protocol stated above for Frontier's Response to DR 05-F, Attachment ("DR 5 Attachment 1 Confidential").

The first three columns in Table 10.3, labeled "City," "PSAP Name," and "PSAP Serving Area" show the location. The final column labeled "Diverse" shows whether the connection is diverse or not. In order to disclose useful information about the extent to which these connections are diverse, and at the

[193] Frontier Response at 6.

same time to protect the network from possible threats, we will redact the first three columns showing location and disclose only the fourth column on diversity.

g. Response to DR 05-F, Attachment ("DR 5 Attachment 3 Confidential")

Staff DR 05-F, discussed above, requested Frontier to provide back-up power standards for Central Office and electronic field equipment. Frontier states that this attachment identifies the number of hours of Central Office battery and/or generator-provided power broken down by CLLI code.[194]

This information is in a table showing which Central Offices have at least 8 hours of back-up power. (Report, at 510-511, Table 10.4.) Information regarding the back-up power at various Central Offices is highly relevant to an analysis of network safety and reliability. Moreover, this table only discloses Central Offices with "at least 8 hours" of back-up power. Because it does not disclose which Central Offices have 8 hours and which offices have more, it does not reveal which Central Offices might be more vulnerable to attack. Therefore, we find that the public interest in disclosure clearly outweighs the public interest in non-disclosure. (Compare AT&T back-up power data below, which is more specific.) Therefore, Table 10.4 should be disclosed.

5.2.2. AT&T DR Responses at Issue

AT&T contends that DR responses 02-A, 05-A, 07-A, 08-A, 09-A and their supplemental DR responses contain critical infrastructure information. To support this claim, AT&T states that, in the course of this examination of AT&T's network infrastructure, AT&T provided the Commission's consultant with extensive and detailed financial, network, and operational information, and that

[194] Frontier Response at 6.

"[p]ublic disclosure of this information … would present a national security risk."[195] AT&T further states that DHS has designated the nation's communications networks, including AT&T's network, as critical infrastructure under 6 U.S.C. § 671(6)(A) & (B).[196] "Information provided to the Commission's consultant includes information on the location of AT&T's critical assets - central offices, remote terminals, etc." and "investment data and customer counts, thus allowing a bad actor to identify, for example, where to strike the AT&T network in order to have the maximum effect."[197]

a. Response to DR 02-A and Supplements: "Facility Deployment and Customer Counts"

AT&T's responses to this data request include a statewide map depicting: (a) "Where AT&T has deployed Fiber to the Premises (FTTP), Fiber to the Node (FTTN), Remote Terminal Digital Subscriber Line (RT-DSL), Central Office Digital Subscriber Line at speeds greater than 14.7 Mbps (CO-DSL>14.7), and Central Office Digital Subscriber Line at speeds less than 14.7 Mbps (CO-DSL< 14.7)" and (b) The location of AT&T's Serving Area Interfaces and Remote Terminals."[198]

AT&T contends that maps showing the statewide locations of AT&T Service Area Interfaces ("SAIs") and Remote Terminals is critical network infrastructure information. AT&T alleges that the release of this mapping would

[195] AT&T Response at 2.

[196] AT&T Response at 2.

[197] AT&T Response at 2.

[198] AT&T Response at 5.

be harmful in that it could provide a comprehensive roadmap for sabotage of AT&T facilities.[199]

The maps that are used in the Network Report include maps showing deployment of facilities by individual wire center (at 98-102, Figures 3.9) and exchange maps for each wire center where staff made site visits (at 569-583, Figures 12.7-12.19).

We agree with AT&T that disclosure of these maps might potentially pose a risk to public safety. We find the public interest in nondisclosure of these maps in the Network Report clearly outweighs the public interest in disclosure at this time. Therefore, we will redact the maps identified above. If, however, later events suggest the need for further disclosures, we may revisit our disclosure determination at that time.

b. Response to DR 05-A and Supplements: "Central Offices and Public Safety Answering Points (PSAPs)"

AT&T's response to DR 05-A includes the following information at issue:

(1) Statewide AT&T Central Office and Public Safety Answering Point (PSAP) Information, including

- Identification of AT&T Central Offices which play a role in serving PSAPs, and the PSAPs associated with each
- Switch type and model broken down by Central Office
- The type of traffic handled by each Central Office playing a role in serving PSAPs (originating vs. overflow 911) and signaling type;

(2) Central Office backup power fuel capacity;

[199] AT&T Response at 6.

(3) AT&T methods and procedures for responding to disaster situations; and

(4) Graphical depiction of 911 routing.[200]

AT&T makes essentially the same argument for nondisclosure of this information as it does for DR 02-A above. AT&T contends that this information includes critical network infrastructure information, the release of which would be harmful. According to AT&T, the identification of Central Offices serving PSAPs and the types of traffic they handle could be used to sabotage critical facilities.[201]

Some of this information was used as background information in the narrative of the Network Report. For example, specific text describes PSAP connection redundancy (at 456); a narrative on routing of 911 calls (at 458); and a general description of AT&T's Disaster First Strike response process (at 485-486). In addition, there is a sample drawing of diverse physical routing (at. 455) and a table showing aggregated totals of AT&T Central Offices hosting PSAPs, and how many are not diverse (at 76, Table 3.4). Because this information is general and aggregated, disclosure does not pose a risk to public safety and it is in the public interest to disclose this information. Therefore, we find that this information should be disclosed.

In addition, AT&T provided tables showing which Central Offices have route diversity (at 457, Table 9.1)[202] and which Central Offices hosting PSAPs have PSAP diversity (at 459-467, Table 9.2). As discussed above in relation to

---

[200] AT&T Response at 7-9.

[201] AT&T Response at 7.

[202] Because this particular table indicates all Central Offices that are diverse, all the Central Office information in the table should be redacted.

Frontier, Table 9.1 only shows Central Offices with route diversity and does not reveal more vulnerable spots; thus, we do not think disclosure would pose a risk to public safety. Therefore, this table should be disclosed without redactions.

In contrast, Table 9.2 reveals which routes are diverse and which are not. Table 9.2 shows the diversity to the Public Switched Network and PSAP diversity. This information, if disclosed, could potentially make the network more vulnerable. Therefore, we will redact columns 1 ("Central Office CLLI") and 2 ("Central Office Name") so that specific locations showing non-diverse routing are not revealed.

AT&T's Central Office backup power availability, listed by each Central Office, is disclosed in the Report. (Report, at 469-481, Table 9.3.) Unlike Frontier's back-up power table, Table 9.3 discloses the specific hours of back-up power for each Central Office. Full disclosure of such information at this time could theoretically pose a risk by allowing a terrorist or saboteur to target the most vulnerable locations, i.e. those with less backup power. We will address this concern by redacting the Central Office identifying information, while disclosing the hours of backup power for each unidentified Central Office. Thus, we will redact the first 2 columns in Table 9.3 labeled "CLLI" and "Central Office Name." The availability of backup power hours is essential to the issue of reliability of the network and is mandated by the FCC. It is in the public interest to allow other parties and the public to see information related to utility compliance with back-up power requirements and overall system reliability. However, if the locations are redacted, public safety will not be jeopardized by disclosing this information.

AT&T methods and procedures for responding to disaster situations are described generally in text with minimal information imparted. (Network

Report, at 485-486.) We do not see any risk to public safety in disclosing the general information on this subject that is included in text of the Report.

The graphical depiction of 911 routing is not included in the report. The report draws on public sources (which AT&T did not provide) to present a drawing of diverse physical routing. Because this drawing is based on public information, it should be disclosed.

c. Response to DRs 07-A, 08-A, and 09-A and Supplements: "Detailed Accounting Data"

AT&T's responses to these data requests include:

(1) Investment data, including

- Land, Buildings, Administrative Assets
- Central Office Transmission Assets
- Cable and Wire Assets

(2) Expense data, including

- Account and High-Level Description
- General Administrative Expenses[203]

AT&T has pages of columns describing each of these categories. AT&T claims confidentiality based on trade secrets for most of this information. However, AT&T also claims that some of this information, if disclosed, would allow a bad actor to target locations where a destructive act could have the greatest impact, e.g., by focusing on locations with newer technologies and/or more recent and higher investments.[204]

In contrast to information and maps showing locations of PSAPs, types of switches, diversity, and backup power, we do not believe that disclosure of

[203] AT&T Response at 10-24.

[204] AT&T Response at 10-21.

investment and expense information poses the same level of security risk. Financial information may show where AT&T has invested resources and even what facilities are newer, but it does not reveal where the network is most vulnerable to a physical attack in terms of disabling the network. On the other hand, a vital public interest favors releasing this information. The amount of money AT&T invested in its network affects service quality and is a primary focus of the Network Study and Network Report. For these reasons, we find that this information should be disclosed.

5.3. Discussion and Analysis of Category 3 Information: CPUC Staff Site Visits to Wire Centers or Central Offices

Category 3 information consists of "[i]nformation and photographs obtained from CPUC Communications Division staff site visits (e.g., outage locations; network facility maps; photographs of equipment inside AT&T and Frontier Central Offices)."[205] Category 3 information is discussed in the Network Report, Chapter 12 (Communications Division Staff Site Visits). CD staff prepared Chapter 12 based on staff's notes, general observations, photographs, and high-level exchange maps the carriers provided in response to data requests.

As background, CD staff chose sites based on the following criteria:

- Areas with high out-of-services numbers;
- Areas with a higher number of subscribers located in urban areas as a comparison to rural wire centers;
- Wire centers with better service quality that are adjacent to poorly performing areas;
- Areas receiving investments from fines imposed by GO 133-D; and,

[205] August 16, 2019 ACR at 3.

- Areas with clusters of outage complaints filed with the CPUC's Consumer Affairs Branch (CAB).[206]

Chapter 12 includes interior and exterior photographs of wire centers that staff took at each site visit. Chapter 12 also includes high-level exchange maps (Figures 12.7-12.1 at 569-583) of each wire center visited that the carriers provided in response to data requests and designated as confidential. *See* discussion *supra*, Category 2.

Chapter 12 also discusses staff's observations at each of the 16 wire centers visited. For each site visit, staff focused on observing the following items:

> 1. *Central Office* – General condition, security and accessibility of building (exterior and interior). Inspection of the following items inside the Central Office (CO): MDF (main distribution frame), switching equipment, ancillary equipment, battery plant, stand-by generator, fuel storage, maintenance logs and cable vault.
>
> 2. *Staffing resources* – Whether Central Office is staffed full-time, part-time or solely "on-demand." Approximate number of Outside Plant resources available in the area, and amount of traveling required.
>
> 3. *Outside Plant network equipment* – Inspection of digital loop carrier equipment in cabinets and associated SAI (Serving Area Interface) cross-boxes, FTTN (fiber to the node) and FTTP (fiber to the premises) equipment (where applicable).
>
> 4. *General Outside Plant* – Inspection of poles, pedestals, cables, splices, pole-mounted cross-boxes and associated facilities. Photographic documentation of damaged plant (cables, terminals, splice cases, pedestals) and temporary fixes.
>
> 5. *Specific inspections of distribution areas* (neighborhoods) with high incidences of out-of-service (OOS) trouble reports, repeated trouble reports and customer complaints.

[206] Network Report at 539-540.

6. *General observation of the population density* of wire center serving area and prevalence of customers located more than 18,000 feet from the Central Office.[207]

In addition to describing staff's observations about the 6 topics above, Chapter 12 includes tables that reflect general information about each of the 16 wire centers: (a) wire center name, (b) ranking, (c) number of lines in the 4Q 2017, (c) whether broadband is available, population in 2010, (d) total square mileage of the Central Office serving area, and (e) designation as rural or urban.[208]

5.4. Carriers' Confidentiality Claims

Frontier requests confidential treatment of a number of photographs taken by staff during site visits that concern the location of specific infrastructure, equipment, or facilities that Frontier states are not publicly available.[209] Frontier claims that such photographs reveal critical infrastructure information, which, if disclosed, could compromise network security," and that "the following photographs taken by staff may be used to help identify the location and specific types of telecommunications infrastructure equipment and facilities that is critical to public safety and connectivity in the area served by Frontier, and their public disclosure could compromise network security…"[210] Frontier once again cites 6 C.F.R. 29.2, and asserts that: "This information was voluntarily provided to the Commission with the expectation of protection from disclosure as

---

[207] Network Report at 541.

[208] Tables 12.3 (Marin County), and 12.4 (Mendocino County), 12.5 (Sutter, El Dorado, and Nevada Counties), and 12.6 (San Mateo and Santa Clara Counties) reflect AT&T's 14 wire centers, and Table 12.7 (Los Gatos) reflects Frontier's two wire centers. Network Report, at 543, 548 554, 560, and 564.

[209] Frontier Response at 9.

[210] *Ibid*.

provided by 6 U.S.C. § 673(a)(1)(E). This information is therefore restricted from disclosure as material specifically precluded from disclosure by statute. See Gov. Code § 6254(k); *see also*, Gov. Code § 6254(e)."[211]

Finally, Frontier asserts that:

> This Critical Infrastructure Information also merits protection under the CPRA's 'balancing test,' both because of the threat to public safety that would be created by disclosure, and because disclosure would facilitate unfair competition. In particular, these photos would provide valuable information to current and potential competitors regarding the engineering and capabilities of Frontier's network and could be unfairly used to facilitate competitive deployment, operations, or marketing efforts. As noted above, there are no countervailing public benefits to making these photos public.[212]

AT&T also contends that interior photographs revealing specific equipment and their location, as well as maps, should not be publicly released. AT&T argues that these photographs are not publicly available and would allow a potential saboteur the ability to preplan destruction of the network to maximize disruption of service to customers. AT&T also alleges that such information constitutes a trade secret.[213]

5.5. Wire Center Interior and Exterior Photographs

There are approximately 60 site visit photographs in the Report, some taken inside and some outside of a wire center. Several inside photos look generic and may be similar to public photographs. Nevertheless, because the public is not permitted access to the interior of wire centers, we believe that these

---

[211] *Ibid*.

[212] *Id*. at 9-10.

[213] AT&T Response at 23-24.

interior photographs might reveal infrastructure information that could be of potential use to those seeking to harm utility facilities.[214] Accordingly, we find it is not in the public interest to publicly disclose these photographs at this time to ensure public safety. In addition, photos of outside generators that are linked to a specific wire center or Central Office should not be disclosed for the same reasons.

We reject assertions that this information is protected from disclosure by 6 U.S.C. § 673(a)(1)(E), FCC Report and Order 04-188, Gov. Code § 6254(k), and Gov. Code § 6254(e), for the same reasons we rejected similar claims regarding Category 1 and Category 2 data. We reject claims that the CPRA balancing test favors nondisclosure based on unfair competition contentions, again, for the same reason we rejected similar contentions in other contexts. We also reject AT&T's contention that "AT&T's competitors do not publicly release comparable information. Consequently, such information is a trade secret …"[215] The actions of AT&T's competitors have no bearing on the trade secret status of AT&T's information.

We instead rest our decision to withhold these photographs at this time entirely on the basis of our own independent balancing of interests for and against disclosure under Gov. Code § 6255(a). We determine that, on the facts of this particular case, the public interest served by withholding photographs which

---

[214] We reject assertions that this information is protected from disclosure by 6 U.S.C. § 673(a)(1)(E), Gov. Code § 6254(k), and Gov. Code § 6254(e), for the same reasons we rejected similar claims regarding Category 1 and Category 2 data. We also reject claims that the CPRA balancing test favors nondisclosure based on unfair competition contentions, again, for the same reason we rejected similar contentions in other contexts. We instead rest our decision to withhold these interior photographs at this time entirely on the basis of our own independent balancing of interests for and against disclosure under Gov. Code § 6255(a),

[215] AT&T Response at 24.

if disclosed could pose a potential risk to the safety of utility facilities clearly outweighs the public interest that would be served by disclosure, since disclosure would shed little additional light on the functional status of the carriers' networks or our regulatory oversight.

On the other hand, we find that the remaining outside photographs depicting outside telephone equipment (cables, poles, etc.) and the exteriors of wire centers or Central Offices, many of which were taken from areas that are accessible to the public, do not pose a public safety risk. Therefore, it is in the public interest to disclose those outside photographs.

5.6. CD Staff's Observations from Site Visits

We find that the parts of Chapter 12 detailing staff's observations concerning the six focus areas discussed above should be made public, with the exception of the following: (1) details of the location and configuration of certain equipment (*e.g.* feeder cables) at each Central Office (Network Report at 543, 549, 556, 565); and (2) specific details about staffing resources at each Central Office (Network Report at 544, 548, 549-550). This level of detail should not be disclosed based on our prior infrastructure safety analysis.

The other information consists of staff's own observations concerning items of great public safety importance related to network reliability and resilience, including but not limited to condition of equipment, backup power capability, broadband options, information provided by employees who approached staff during site visits and information from employees designated to answer staff's network study questions. We find that staff's observations should be disclosed.

5.7. Exchange maps (Figures 12.7-12.21)

AT&T and Frontier provided these high-level exchange maps to staff in response to Network Study data requests. Based on our infrastructure safety discussion regarding certain Category 2 data responses, we find that these maps should not be disclosed at this time. These maps show the precise boundaries of individual wire centers, with sufficient detail regarding location of utility facilities to be of potential use to those seeking to harm utility facilities. As discussed below, there is more detailed information in the Network Report, including the tables in Chapter 12, that would provide the public with sufficient information to understand the Report.

5.8. Tables in Chapter 12 Summarizing Wire Center Information Should Be Made Public

All the tables in Chapter 12 should be made public. Most of the wire center information in these tables is already public[216]: the cities and counties in which wire centers are located, the population, square mileage, rankings and number of lines are based on public service quality report data (4th Quarter, 2017), and whether an area is designated as rural or urban. Further, whether broadband is or is not available in a particular wire center area is not a secret.

5.9. Gov. Code §6255(a) CPRA Balancing Test Claims

We disagree with Frontier's contention that the Category 3 photographs and other information for which Frontier seeks confidential treatment "warrant protection under the CPRA's balancing test … because disclosure would facilitate unfair competition"[217] for the same reasons we disagreed with similar claims regarding Category 1 and Category 2 information.

---

[216] *See e.g.*, https://www.stuffsoftware.com/cofindernew.aspx; *see* also, FN 122.

[217] Frontier Response at 10.

We also disagree with Frontier's contention that "there is no countervailing public benefit to making these photos public,[218] and with Frontier's implicit assumption that the identification of a public interest is required. Neither the Cal. Const, Art. 1, § 3, nor the CPRA, require a "countervailing public benefit" to justify disclosure of government records in the face of an information submitter's confidentiality claims; rather, a public interest in the disclosure of records relating to "the conduct of the people's business" is presumed, and agencies wishing to withhold records on the basis of the § 6255(a) balancing test must themselves identify public interest served by nondisclosure which, on the facts of the particular case, clearly outweighs the public interest served by disclosure.

We do agree, however, that, on the facts of this particular case, and in an abundance of security-related caution, the public interest that would be served by withholding certain photographs of Frontier's facilities that might, if disclosed, be of some use to those seeking to harm utility facilities clearly outweighs the public interest that would be served by disclosure at this point in the proceeding. Disclosure of photographs of the interiors of certain of Frontier's Central Offices would appear to shed minimal light on the functional status of Frontier's network, or on the Commission's oversight of that network.[219]

If, however, later events suggest the need for further disclosures, we may revisit our disclosure determination at that time. Our specific disclosure decisions are discussed above, with reference to specific Category 3 information in the Report.

---

[218] *Ibid*.

[219] As noted earlier, photographs of the exteriors of many AT&T and Frontier Central Offices are readily available to the public; *see*, e.g., www.co-buildings.com/ca.

6. Discussion and Analysis of Category 4 Information: Annual Financial Reports and Other Financial Information

Category 4 information, discussed in Chapters 7 (AT&T Corporate and California ILEC Investment Policies) and 8 (Verizon/Frontier Corporate and California ILEC Investment Policies), consists of "[a]nnual financial reports filed by AT&T California, Verizon California, and Frontier California that conform to the Federal Communications Commission's Automated Reporting Management Information System ("ARMIS") reporting requirements. ARMIS is a reporting protocol which was adopted by the FCC in 1987 to collect financial and operational data from the larger carriers.[220] ARMIS Reports cover information regarding finances, operations, service quality, customer satisfaction, switch downtime, infrastructure, and usage.

Significantly, ARMIS information was available to the public and used in many Commission proceedings.[221] In 2007, the FCC decided to cease requiring ARMIS reporting by ILECs subject to FCC rate cap rather than rate of return regulation. The CPUC has continued to require ARMIS reports to be filed by Uniform Regulatory Framework Incumbent Local Exchange Carriers (ILECs).[222] Because the issues related to the disclosure of ARMIS reports are almost identical to those related to the disclosure of USOA account specific financial and infrastructure information provided in Category 2 data request responses, we address both matters together.

Generally, the Network Report utilizes ARMIS data and data request response data in two ways. First, it simply provides the data drawn from the

---

[220] *See e.g.*, D.04-09-063 at 37, fn. 27.

[221] *See e.g.*, D.02-09-049; D.04-03-013, D.01-12-021, D.04-09-053.

[222] August 16, 2019 ACR at 3.

ARMIS forms and data request responses in tabular form, as well as by using numerical data drawn from those documents in the text of the Report. Mathematical calculations are also conducted on such data to generate percentages (or other data), often in conjunction with information from other sources. For example, Table 7.1 at page 375 provides AT&T Inc.'s operating revenues (which are publicly available in its annual reports), AT&T California's operating revenues (drawn from ARMIS Form 43-01), as well AT&T California's operating revenues as a percentage of AT&T Inc.'s operating revenues (a calculation).

The report also uses the ARMIS data to inform its narrative analysis. The bulk of the report consists of narrative text that describes the consultants' analysis and conclusions regarding the subject companies.

The consultants' analysis and conclusions are of great public value. While competitors could theoretically scour the report's narrative for clues about the companies' strategies, whatever economic disadvantage this would bring is outweighed by the public interest in disclosing the analysis and conclusions, so that the public can understand the overarching ramifications of the Network Report.

Beyond that, the Commission previously disclosed the narrative portions of the summary of the report (Chapter 1), as well as most of the text from the table titles (Table of Contents). To the extent that such text is repeated within the report, it clearly may be disclosed as it is already public. Narrative analysis beyond what has already been disclosed in the summary and table of contents is also subject to disclosure, as it supports and complements the public analysis and conclusions. Indeed, there is no valid basis for publishing only a portion of the narrative analysis of the ARMIS data. Even if there were, the CPRA balancing

test analysis supporting the disclosure of the narrative within the Chapter 1 Summary and Table of Contents would be the same. The public interest in nondisclosure does not clearly outweigh the public interest in disclosure.

It is also worth noting that while the consultant ETI may have reviewed the raw ARMIS data in developing conclusions set forth in the Network Report, the narrative analysis of what that data means represents the work product of ETI on behalf of the Commission, not of AT&T or Frontier. Moreover, the analysis presents information that has been aggregated and therefore does not reveal underlying information.

We discuss below the specific ARMIS reports which AT&T and Frontier assert should be afforded confidential treatment. We then review the carriers' trade secret and CPRA balancing test confidentiality assertions and make our disclosure determinations. This discussion will also include analysis of the USOA accounts financial information from Category 2.

6.1. ARMIS Reports at Issue

6.1.1. ARMIS Form 43-01

ARMIS Form 43-01 is the Annual Summary Report. Relevant data from such reports include total California specific operating revenues. Frontier states that ARMIS Form 43-01 includes "data by each applicable FCC revenue, expense and investment account, including nonregulated revenues, expenses and investments, as well as granular access line information and demand analysis by type of customer."[223] Both AT&T and Frontier argue that the aggregated information in ARMIS Form 43-01 constitutes a trade secret. AT&T asserts that it does not disclose "California-specific information and AT&T's competitors do

[223] Frontier Response at 11.

not reveal similar California-specific data publicly."[224] Frontier also seeks confidential treatment of this entire report.[225]

6.1.2. ARMIS Form 43-02

ARMIS Form 43-02 includes the operating results for the USOA. AT&T seeks confidential treatment for Table B-1 (Balance Sheet Accounts), which shows "AT&T California's investments (plant additions, retirements, and end of year balances) by specific categories of plant, including general support assets, central office assets (switching and circuit electronics), and outside plant cable facilities."[226] AT&T also seeks confidential treatment for Table I-1 (Income Statement Accounts), Table B-2 (Statement of Cash Flows), Tables B-3, B, and I-2 (regarding affiliates), Tables B-5 and B-6 (regarding Depreciation), Table I-6 (Special Charges), and Table I-7 (Donations or Payments for Services Rendered by Persons Other Than Employees).[227]

Regarding ARMIS Form 43-02, Frontier seeks confidential treatment of Table C-5 ("to the extent that it identifies and contains a description of contracts or agreements with third parties"), Table B-1 ("granular balance sheet information"), Table B-2 ("to the extent it contains detailed statements of cash flows"), Table B-3 ("to the extent it contains information related to investments in affiliates and other companies"), Table B-5 ("granular analysis of specific accounts in accumulated depreciation"), Table B-7 ("account-specific information and granular analysis of the bases of charges for depreciation"), Table B-10 ("payments made to or received from affiliates"), Table I-1 ("granular income

[224] AT&T Response at 25.

[225] Frontier Response at 11.

[226] AT&T Response at 25.

[227] AT&T Response at 25-29.

statement on an account-specific basis"), Table I-2 ("costs and prices for services purchased from or sold to affiliates"), and "the portion of Table I-7 identifying payments made to specific contractors."[228] Both AT&T and Frontier assert that the information indicated above is a trade secret.[229]

6.1.3. ARMIS Form 43-03

ARMIS Form 43-03 consists of a joint cost report. AT&T seeks confidential treatment for Table B-1 (Balance Sheet Accounts), Table I-1 (Income Sheet Accounts), and the portions of Table C-5 "which disclose important changes in service[.]"[230] AT&T emphasizes that "[t]he portion of Table C-5 which discloses important contracts or agreements is a veritable roadmap to AT&T's interconnection business with Competitive Local Exchange Carriers."[231] AT&T does not seek confidential treatment for Table C-3 (Respondent Corporate Information), which lists "AT&T California's board of directors and general officers of the carrier."[232] Frontier seeks confidential treatment of the entirety of ARMIS Form 43-03.[233]

Both AT&T and Frontier assert that the information indicated above is a trade secret (with the exception of AT&T's Table C-3).[234]

6.1.4. ARMIS Form 43-07

ARMIS Form 43-07 is an infrastructure report. AT&T requests confidential treatment of Table I (Switching Facilities), which includes "data on the number

---

[228] Frontier Response at 11.

[229] AT&T Response at 25-29; Frontier Response at. 11-12.

[230] AT&T Response at 29.

[231] AT&T Response at 30.

[232] AT&T Response at 30.

[233] Frontier Response at 12.

[234] *See* AT&T Response at 29-30; Frontier Response at 12.

and types of switching facilities AT&T California maintains across the state" and Table II (Transmission Facilities), which contains "AT&T California's outside copper and fiber cable, as well as central office terminations."[235] Frontier requests confidential treatment for the entire ARMIS Form 43-07 Report, which contains "granular information concerning switching equipment transmission facilities, equipment and facility capabilities, and access lines and minutes."[236]

Both AT&T and Frontier assert that the information indicated above is a trade secret.[237]

6.1.5. ARMIS Form 43-08

ARMIS Form 43-08 is an operating data report. AT&T requests confidential treatment for Table I.A (Outside Plant Statistics – Cable and Wire), Table I.B (Outside Plant Statistics – Other), Table II (Switched Access Lines In Service), Table III (Access Lines In Service By Customer), and Table IV (Telephone Calls).[238] AT&T asserts that the information indicated above is a trade secret.[239]

6.2. Carriers' Confidentiality Claims Concerning ARMIS Reports and Category 2 Financial Information Obtained from Network Study Data Request Responses

Frontier states that "[t]he ARMIS reports contain competitively-sensitive financial materials, and Frontier understands that these data have been consistently protected as confidential for competitive companies when submitted

---

[235] AT&T Response at 30-31.

[236] Frontier Response at 12.

[237] AT&T Response at 30-31; Frontier Response at 12.

[238] AT&T Response at 31-34.

[239] *Ibid*.

to the Commission in connection with annual reporting requirements."[240] Frontier asserts, with regard to the ARMIS Reports, that the information identified above is protected as a trade secret, citing Evid. Code § 1060, which Frontier incorporates as a ground for protection under Gov. Code § 6254(k).

To support its trade secret claim, as with Category 2 account specific information, Frontier argues that the detailed financial, investment, and access line information in the ARMIS reports reflects a "pattern," "compilation," or "process" which derives economic and competitive value from not being known to the public and kept from Frontier's competitors, and Frontier consistently maintains this information as confidential. Frontier further claims that"[t]his type of information would be useful to a competitor and harmful to Frontier if used to direct current and potential competitors' deployment, operations, or marketing efforts. If made public, these trade secrets would be compromised, and their use could facilitate unfair competition."[241]

Frontier argues that this information also merits protection pursuant to the CPRA balancing test. It claims that "[t]he disclosure of account-specific financial, investment and access lines data from Frontier's and Verizon's operating companies would undermine competition in the overall telecommunications market" and "[a]ny perceived public benefit associated with the disclosure of this type of information is clearly outweighed by the extensive harm caused to competitors and competition that would occur from forcing Frontier to disgorge this information through the regulatory process and reveal it to its competitors.

[240] Frontier Response at 2.

[241] *Ibid*.

See Cal. Gov. Code § 6255(a)." In other words, according to Frontier, this would undermine the functioning of a competitive market and harm consumers.[242]

Frontier makes similar assertions with regard to account-specific information in various Category 2 data request responses, with one difference being its CPRA balancing test contention that: "This balancing test is appropriately employed to protect competitive information of a regulated entity from disclosure because a strong public interest exists in encouraging vigorous competition for the benefit of consumers and potential employees."[243]

AT&T asserts that the ARMIS reports are confidential pursuant to California Government Code § 6254(k), California Evidence Code § 1060, California Civil Code § 3426 *et seq.* and 18 U.S.C. Chapter 90 *et seq*.[244]

AT&T's and Frontier's confidentiality contentions concerning ARMIS Reports are similar to confidentiality assertions made with regard to account specific information in various Category 2 data request responses. Therefore, we consolidate our response to the carriers' trade secret claims and to Frontier's assertion that such information also warrants confidential treatment pursuant to the CPRA balancing test described earlier.[245]

6.3. Discussion of Trade Secrets Claims

"Cal. Gov. Code § 6254(k), provides the Commission may withhold information if the disclosure of information is prohibited by federal or state law."[246] Parties citing section 6254(k) "must also cite the applicable statutory

---

[242] Frontier Response at 12.

[243] *Id*. at 8.

[244] AT&T Response at 26.

[245] Frontier Response at 12.

[246] D.17-09-023 at 44.

provision and explain why the specific statutory provision applies to the particular information."[247]

As previously discussed, a trade secret must: 1) be information of the trade secret asserter; 2) be secret, *i.e.*, not generally known to the public or to those who could make economic use of it, 3) have independent economic value by virtue of being secret, and 4) the subject of efforts by the trade secret owner that are reasonable under the circumstances to maintain their secrecy.[248] Trade secret asserters must be prepared explain their trade secrets in ways that allow them to be distinguished from information available elsewhere, or information that otherwise does not fall within a category of information that may be considered a trade secret. They must also be prepared to explain what efforts they have made that are reasonable under the circumstances to maintain the secrecy of the trade secret.[249]

Evidence Code § 1060 provides that the owner of a trade secret can refrain from disclosing its trade secret and can prevent another from disclosing that trade secret with a fraud/injustice exception.[250] However, voluntary disclosures may waive this protection.[251] As previously noted, "secrecy" is a basic requirement for trade secret status, and the disclosure of "trade secrets" to those who have no obligation to keep the information secret, generally eliminates the

---

[247] GO 66-D, § 3.2(b).

[248] Civ. Code § 3426.1(d).

[249] Civ. Code § 3426.1(d).

[250] Evid. Code § 1060.

[251] *See Stadish v. Superior Court*, 71 Cal.App.4th 1130 (Cal. App. 2d Dist. Apr. 30, 1999); *see* also, fn. 61, *supra*.

ability of the trade secret holder to assert that the information is subject to the trade secret privilege or otherwise protected from subsequent disclosure.[252]

While the carriers have identified specific code sections that they contend prohibit disclosure, their responses do not establish why the identified data, as used in Network Report, would be subject to the cited provisions. For example, they have not explained why they believe account-specific financial and infrastructure information provided in response to detailed government mandates is a "pattern design, compilation," etc. of *theirs* (*see* Civ. Code § 3426.1(d)(1)). Nor have they explained why such information would acquire trade secret status now, when ARMIS information was available to the public in the past and used in many Commission proceedings.[253]

The carriers also failed to explain what economic value such information has for them by virtue of being secret, given the absence of any reference to specific competitors that might make use of the information to the utilities' economic detriment (§ 3426.1(d)(2)). They failed to detail what steps they have taken that are "reasonable under the circumstances" to maintain the secrecy of the information.[254]

The carriers' responses fail to explain why withholding such information from the public in the context of the Network Report, which is focused on network performance issues that may be a result of utility investment practices,

---

[252] *See e.g., Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984); *In re Providian Credit Card Cases*, *supra*, at 881, (2002).

[253] *See, e.g.*, D.02-03-049, D.04-03-013, D.04-09-063, D.01-12-021, D.07-04-019 (Order Denying Petitions to Modify D.01-12-021), at 6: "If the OOS reporting requirement is eliminated, consumers will still have access to data regarding OOS intervals because all carriers include their information in their ARMIS reports filed with the FCC, which are publicly posted on the Internet."

[254] I*bid*.

would not work injustice (*see* Evid. Code § 1060) by limiting the ability of the Commission to conduct this proceeding in a fully open and transparent manner. Finally, the parties have not established that the Commission is expressly prohibited from disclosing the cited ARMIS information. We elaborate below.

Again, we are not saying that information submitted by regulated entities can never constitute trade secret information, but rather that the carriers have in this case failed to prove to our satisfaction that the submitted information meets all the elements of the trade secret definition in Civ. Code § 3426.1(d) and that they are entitled to assert the conditional Evid. Code § 1060 trade secret privilege.

6.3.1. Account Data Prepared and Reported in Formats Created and Mandated by Regulatory Agencies Are Not Trade Secrets

We do not consider the account data provided in Category 2 responses to data requests and referenced in the Network Report to be the trade secrets of AT&T and Frontier. Most of the utility account information summarized and analyzed in the Network Report is based on data from accounting systems and categories developed by government agencies, rather than the carriers' own independent creative efforts and hard work. Further, the discussion and analysis in the Report itself reflects the work of ETI, rather than the carriers under review. It is not clear how ARMIS reports and other USOA based accounting information provided in Category 2 responses to data requests would fall within the first element of the Civ. Code § 3426.1(d) definition of a trade secret.

The accounting data at issue here was provided in organizational categories developed by the FCC for regulatory purposes, and in formats dictated by the FCC and the Commission, and thus does not reflect a pattern, design, compilation, etc., the carriers developed. Pub. Util. Code § 792 states:

> The commission may establish a system of accounts to be kept by the public utilities subject to its jurisdiction, or classify such public utilities and establish a system of accounts for each class, and may prescribe the manner in which such accounts shall be kept. It may also prescribe the forms of accounts, records, and memoranda to be kept by such public utilities, including the accounts, records, and memoranda of the movement of traffic as well as the receipts and expenditures of moneys, and any other forms, records, and memoranda which in the judgment of the commission may be necessary to carry out any of the provisions of this part.[255]

The specific numbers and other information AT&T and Frontier provided in ARMIS reports and elsewhere have meaning primarily because of the context in which they were provided - data systems and reporting formats designed and developed by regulatory agencies – the Commission and the FCC.

In 1935, the FCC established the Uniform System of Accounts (USOA) to facilitate its regulatory mission set forth in 47 CFR § 31. The USOA was revised and expanded in 1986, with 47 CFR § 32 superseding 47 CFR § 31.[256] The USOA system gave management and regulators a consistent tool to maintain and review financial information.[257] Specific USOA account titles and numbers are

---

[255] Pub. Util. Code § 793 states: "The system of accounts and the forms of accounts, records, and memoranda prescribed by the commission for corporations subject to the regulatory authority of the United States, shall not be inconsistent with the systems and forms from time to time established for such corporations by or under the authority of the United States. Nothing in this section or Section 794 shall affect the power of the commission to prescribe forms of accounts, records, and memoranda covering information in addition to that required by or under the authority of the United States."

[256] 47 CFR § 32.

[257] 47 CRFR § 32.1 Background, states in part: "The revised Uniform System of Accounts (USOA) is a historical financial accounting system which reports the results of operational and financial events in a manner which enables both management and regulators to assess these results within a specified accounting period. The USOA also provides the financial community and others with financial performance results. In order for an accounting system to fulfill these

associated functional categories of investments and activities, including gross additions, retirements, depreciation, telecommunications plant in service, among other categories, with much of the information maintained on an individual wire center level.

In 2017, the FCC decided that "price cap ILECs" subject to FCC price cap rather than rate of return regulation would no longer be required to maintain separate USOA accounting records after 2017.[258] The FCC Order making this change expressly states that: "Nothing in this order precludes a state or regulatory agency, … from requiring a carrier to maintain the Class A accounts or otherwise maintain the USOA."[259] FCC Commissioner Mignon L. Clyburn, in a *Statement Approving in Part and Concurring in Part*, stated that:

> So to those carriers who advocate for decreased regulatory burdens, let me assure you: I am with you. However, the next time this Commission or a state commission asks for cost data, to support a rulemaking, investigate a complaint, or bring an enforcement action, I hope we do not hear protestations that the request is too burdensome because the data is not kept in the format that the FCC or state commission need.[260]

Carriers subject to Commission USOA accounting and financial reporting requirements were required to maintain regulatory accounting records in a

---

purposes, it must exhibit consistency and stability in financial reporting (including the results published for regulatory purposes). Accordingly, the USOA has been designed to reflect stable, recurring financial data based to the extent regulatory considerations permit upon the consistency of the well-established body of accounting theories and principles commonly referred to as generally accepted accounting principles (GAAP)."

[258] *I/M/O Comprehensive Review of the part 32 Uniform System of Accounts*, WC Docket No. 14-1130; *Jurisdictional Separations and Referral to the Federal-State Joint Board*, CC Docket No. 80-286, *Report and Order*, FCC 17-15, rel. February 24, 2017.

[259] *Id.* at 7, fn. 52.

[260] *Id*. at 34.

manner the FCC established and mandated, and to file reports in formats created and mandated by the FCC and the Commission.[261]

The Commission continues to require ARMIS reports from ILECs subject to URF rather than rate of return regulation, and such reports continue to have value for regulatory purposes. As D.09-07-019 notes:

> The Commission has a statutory duty to ensure that telephone corporations provide customer service that includes reasonable statewide service quality standards, including, but not limited to, standards regarding network technical quality, customer service, installation, repair, and billing.[28] (*See*, *e.g.*, Pub. Util. Code §§ 709, 2896 and 2897.)[262]

With increasing concerns regarding potential disruptions of telecommunications services resulting from wildfires, natural disasters, or other causes, the strength and resiliency of communications networks is of vital importance to the Commission, and any information that may shed light on factors relating to such issues is significant and important.

The Commission's regulatory responsibilities require it to collect and use information from utilities; utilities subject to our regulation must be prepared to provide it, and such information is widely utilized in our proceedings. Frontier and AT&T state that neither they nor their competitors make such account-

---

[261] 47 CFR § 32. 47 CRFR § 32.1 Background, states in part: "The revised Uniform System of Accounts (USOA) is a historical financial accounting system which reports the results of operational and financial events in a manner which enables both management and regulators to assess these results within a specified accounting period. The USOA also provides the financial community and others with financial performance results. In order for an accounting system to fulfill these purposes, it must exhibit consistency and stability in financial reporting (including the results published for regulatory purposes). Accordingly, the USOA has been designed to reflect stable, recurring financial data based to the extent regulatory considerations permit upon the consistency of the well-established body of accounting theories and principles commonly referred to as generally accepted accounting principles (GAAP)."

[262] D.09-07-019 at 12.

specific information public, but neither Frontier nor AT&T explain what actual steps they do take to keep such information secret, falling far short of the type of "reasonable steps" information generally provided in trade secret misappropriation litigation.

We note that there may at times be differences between ARMIS report accounting information and other carrier data. In D.04-09-063, for example, the Commission stated that: "While SBC-CA's filings and workpapers traced input costs to SBC-CA's internal account codes, we could not match this internal accounting data to SBC-CA's publicly available cost data, i.e., ARMIS filings."[263] ARMIS reports include information based on USOA accounting requirements in formats mandated by regulatory agencies for regulatory purposes.

While ARMIS accounting information may vary from other accounting systems created and maintained by carriers on their own initiative, there are limits on the ability of utilities to maintain independent accounts where the Commission has prescribed accounting forms and records. Pub. Util. Code § 794 states:

> The commission may, after notice, and hearing if requested within 15 days after receipt of notice, prescribe by order the accounts in which particular outlays and receipts shall be entered, charged, or credited. Where the commission has prescribed the forms of accounts, records, or memoranda to be kept by any public utility for any of its business, it is unlawful for such public utility to keep any accounts, records, or memoranda for such business other than those so prescribed, or those prescribed by or under the authority of any other state or of the United States, except such accounts, records, or memoranda as are explanatory of and supplemental to those prescribed by the commission.

[263] D.04-09-063 at 26, FOF 9.

Accordingly, we find that the carriers have failed to demonstrate that the information contained in the Network Report constitutes a design, formula, or compilation or other information falling within the definition of a trade secret in Civ. Code § 3426.1(d).

As FCC Commissioner Mignon pointed out, even though the FCC no longer requires the maintenance of USOA accounting records by many carriers, carriers are on notice that in the future, the FCC or a state regulatory agency could ask for cost data for a variety of regulatory purposes, and carriers should be sure to maintain records in a responsive format. This proceeding involves such requests for USOA accounting records, and for ARMIS Reports which include information based on USOA accounts.

As noted earlier, the Evid. Code § 1060 trade secret privilege is a conditional privilege that can only be asserted where allowance of the privilege would not tend to conceal fraud or otherwise work injustice.[264]

Thus, even if the account-specific financial and infrastructure data in ARMIS Reports and data request responses provided to the Commission and summarized in the Report were trade secrets – a contention with which we do not agree– it is not appropriate that any trade secret privilege be asserted here. Asserting the privilege here would substantially and unfairly disadvantage parties participating in this proceeding and Commission proceedings generally, and the public, by limiting their ability to review information essential to a fair resolution of a proceeding addressing telecommunications network service quality, safety, and reliability, and prevent the public from understanding the

[264] *See, e.g., Uribe v. Howie*, (1971) 19 Cal.App.3d 194, 205-207, 210-211.

status and functions of a telecommunications network ever more central to their lives.[265]

6.4. The CPRA Balancing Test Favors Disclosure

As explained above, the CPRA balancing test in Gov. Code § 6255(a), states that an agency may withhold information in response to records requests if it determines that, "on the facts of the particular case, the public interests served by nondisclosure clearly outweigh the interests that would be served by disclosure."

We are not persuaded by Frontier's contention that our balancing of interests for and against disclosure under the "balancing test" would lead us to determine that, on the facts of this particular case, the public interest served by withholding the account-specific financial and infrastructure records would clearly outweigh the aforementioned public interest served by disclosure. Frontier asserts, without specific facts, that certain disclosures might "undermine competition in the overall telecommunications market."[266] This general assertion is inadequate to persuade us to find that, on the facts here, the public interest that would be served by withholding information from the public clearly outweighs the public interests that would be served by disclosure.

---

[265] *Bridgestone/Firestone*, *supra*, discusses several factors involved in a judicial determination whether disclosure of trade secrets should be ordered in civil litigation, and whether protective orders or other options could preserve the interests of a trade secret holder while still serving the needs of parties for essential information. Procedures set forth in that case are not applicable to the Commission. (D.06-01-047, *Ordering Modifying and Denying Rehearing of Decisions 04-05-017 and 04-05-018*, at 35-36). We note that the needs of the public, not just the parties, for information regarding the networks of AT&T and Frontier makes it unlikely that protective orders would provide sufficient access to information essential to this proceeding, even if the data at issue were considered to be a trade secret, which we do not believe.

[266] Frontier Response at 12.

Frontier contends that there is a public interest in avoiding unfair competition, and disruption of the normal functioning of the market.[267] We note that Frontier fails to explain how the market could be disrupted by disclosure, beyond asserting that the disclosure of account-specific and other information that its unnamed competitors do not disclose to the public would create an uneven playing field in a competitive marketplace.[268] We are unpersuaded by this argument, given that a competitive market presumes that consumers are well-informed. It is the intent of the legislature that consumers be well-informed, so that they may make informed choices regarding telecommunications services and providers.[269]

Disclosure is favored here because the Network Study is intended to explore, among other things, why service quality remains inadequate despite our prior presumption that a competitive market exists. Disclosure would have the benefit of motivating carriers to provide higher quality and more reliable service.

We previously explained that the potential for disclosure to result in competition is not something we view adversely. As we also noted earlier, Frontier and AT&T brought themselves to our attention by providing services that are not in compliance with our service quality standards, to the point where we initiated this Network Study with its intentional close look at network investments and operations.

Thus, we reject the carriers' contentions that disclosure of this account information would result in any unfair competition or harm to the overall communications marketplace because we are not disclosing similar information

---

[267] *Ibid*.

[268] *Id*. at 8-9.

[269] *See e.g.,* P.U. Code § 2896.

regarding other URF ILECs or other potential competitors subject to our regulation.

In our view, Frontier's balancing of interest assertions appear to be primarily based on a fear of increased competition from unnamed competitors, with its potentially negative impact on Frontier's individual corporate well-being, rather than on a reasoned argument that the public itself would be better off not seeing the information at issue. As both D.17-09-023 and GO 66-D acknowledge, the CPRA balancing test claim must be based on more than purely economic self-interest.

We find, on the particular facts of the Network Study, that, in addition to the public interest in information concerning the conduct of the people's business – here, our regulatory oversight of two communications networks – the disclosure of the account data in the Report will greatly assist the Commission, parties to this proceeding, and the public in understanding the state of the network facilities and operations of AT&T and Frontier during the 8-year study period ending in 2017. The upshot of this effort is that both the good and the bad can be explored in order to learn why these carriers for so many years have had difficulty meeting our service quality and reliability requirements, whether service quality and reliability is better in some areas than others, and, if so, why. This information will provide us the path to explore other possible ways to improve the performance of these carriers.

With our attention focused on these carriers, and the need for disclosure of detailed information in assessing problem areas in their networks and identifying potential solutions with stakeholders, we do not see disclosure of accounting information related only to these carriers as inherently unfair or prejudicial.

We note that the latest data summarized in the Network Report dates from 2017, while the rest of that data is even older. We have long recognized that the sensitivity of proprietary financial information generally declines over time, and therefore routinely provide confidential treatment for such information for only a limited time period, typically two years.[270]

To the extent AT&T and Frontier assert that competitors could use the information to detect investment trends over time, we note that such general trend information is available in standard SEC reports and similar resources.

We are not persuaded by the carriers' arguments that the public benefits served by nondisclosure and continued secrecy of this information have real benefits to the public. The fact that similar data is not disclosed by potential competitors and, is therefore not available to AT&T and Frontier, is not compelling. It is AT&T and Frontier's failure to comply with regulatory requirements that necessitates the disclosure of this accounting information in order to for the Commission and parties to adequately address the issues raised in the Network Study.

We note that the CPRA does not include a specific exemption for records, which if disclosed, could place a Commission-regulated entity at an unfair business disadvantage. If competitively sensitive information fairly falls within the statutory definition of a trade secret and is subject to a trade secret privilege assertion allowed by Evid. Code § 1060, an agency may withhold the information pursuant to Gov. Code § 6254(k).[271] But, if an agency such as the Commission

[270] See *e.g.* Decision 01-05-062. _____

[271] The agency should first determine if the information is in fact a trade secret, and then engage in the balancing of interests for and against disclosure as described in *Uribe v. Howie*, supra, to determine if assertion of the Evid. Code § 1060 is allowed, or if assertion of the privilege would tend to conceal fraud or otherwise work injustice. (Civ. Code § 3426.1(d), Evid. Code § 1060.)

does not agree that information which a regulated entity wishes to keep from the public is in fact a protectible trade secret, then the information submitter's competitive disadvantage and unfair competition contentions may be addressed under the Gov. Code § 6255(a) balancing test.

Gov. Code § 6255(a) requires an analysis whether, on the facts of the particular case, the public interest that would be served by the agency's withholding the information from the public clearly outweighs the public interest that would be served by disclosure. An information submitter's competitive disadvantage and unfair competition fears may be considered matters involving private corporate economic interests, rather than truly public interests, and thus may not persuade the agency that the public's interest in not having access to information clearly outweighs the public's interest in having access to the information.[272] Such is the case here.

Based on the foregoing analysis, we conclude that the data drawn directly from the ARMIS Forms, and derivative computations of that data, included in the Network Report shall be open to the public because the carriers have failed to demonstrate that the information is a protectible trade secret or the carriers' interests in withholding the information outweighs the public interest in disclosure.

7. Conclusion

The Network Report was entered into the record of this proceeding under seal due to the confidentiality claims raised by AT&T and Frontier pursuant to GO 66-C or 66-D and Pub. Util. Code 583, as discussed above. The Commission

[272] Again, we note that if carriers feel competitors are engaged in unfair business practices or unfair competition, they may seek remedies through Bus. & Prof. Code § 1700 *et seq*. and § 17200 *et seq*.

has now evaluated the validity of these claims. We conclude that a limited subset of Category 2 and Category 3 information, as discussed above, that contained information that could pose a security risk if disclosed, shall be redacted. Such information appears in the following Chapters: 3, 5, 6, 7, 8, 9, 10, and 12. Chapters 1, 2, 4, 11 and the Table of Contents do not contain information that warrant confidential treatment and staff shall make available these Chapters and the Table of Contents in their entirety on the Commission's website, within 30 days of the effective date of this decision. Staff will make available Chapters 3, 5, 6, 7, 8, 9, 10, and 12 in appropriately redacted form consistent with this decision within 30 days of the effective date of the decision.

8. Comments on Proposed Decision

The proposed decision of the Commissioner in this matter was mailed to the parties in accordance with Section 311 of the Public Utilities Code and comments were allowed under Rule 14.3 of the Commission's Rules of Practice and Procedure. Comments were filed on November 9, 2020 by AT&T, Frontier, CTIA – The Wireless Association, and The Utility Reform Network, Greenlining Institute, The National Consumer Law Center, and Center for Accessible Technology (collectively "Joint Consumers"), and reply comments were filed on November 16, 2020 by AT&T and Frontier jointly, Joint Consumers, and California Cable and Telecommunications Association.

We have considered all comments. In response to comments, we have made changes to the decision to clarify certain aspects of our analysis regarding trade secrets. We have modified findings and conclusions of law to be consistent with those changes to the trade secret discussions in the decision.

The industry comments, including AT&T, Frontier, CTIA, and CCTA, appear to misconstrue the proposed decision's trade secret analysis in raising

concerns that it would apply to a broader context beyond the Network Report. We clarify that the adjudication of confidentiality claims is generally done on a case-by-case basis, as was the case here. And, on the facts presented, we find that AT&T and Frontier failed to satisfy their burden of proof concerning their trade secret, critical infrastructure, and CPRA balancing test confidentiality claims.

AT&T's comments disagree with the proposed decision finding that AT&T's information provided per GO 133-D, Commission data requests, and the ARMIS reporting requirements do not constitute AT&T's trade secrets. AT&T's comments attempt to demonstrate how this information meets all the elements of a trade secret, but that is what it should have done when it first submitted the information at issue. It did not. At the time that AT&T submitted the information to the Commission, it did not explicitly allege in the accompanying confidentiality declarations that the information should be protected as trade secrets under Cal. Evidence Code section 1060 et. seq. or Civil Code section 3426. That undermines the credibility of AT&T's trade secret claim here. As discussed in the decision, AT&T's response to the August 2019 ACR did not overcome its burden of proof either. AT&T's comments are thus unpersuasive.

Notwithstanding its disagreements with the proposed decision, AT&T does acknowledge that the proposed decision's conclusions to release most of the information in the Network Report were properly based upon the public interest balancing test. Therefore, AT&T does not contend that the Network Report should be further redacted.

Frontier's comments similarly take issue with the proposed decision's trade secret analysis and conclusion that the information contained in the Network Report are not Frontier's trade secrets. As with AT&T, Frontier had

failed to meet its burden of proof regarding this claim, and its response to the 2019 ACR did not overcome that burden. As with AT&T, at the time Frontier submitted the information at issue, it did not cite to the trade secret statutes. Instead, Frontier claimed at the time, in its confidentiality declarations, that releasing the information would put it at a competitive disadvantage. Such broad statements do not in itself prove a trade secret. The decision explains in great detail why this claim has no merit, and therefore we were not persuaded by Frontier's comments. Though Frontier disagrees with the proposed decision's trade secret analysis, it does not object to disclosing information in the Network Study that it alleges are trade secrets. Frontier acknowledges that due to the passage of time and the manner in which some of the materials have been excerpted in the Network Study, Frontier does not oppose the decision to release some of the materials made public in the proposed decision.

We reject Frontier's request for further redactions to the Network Report concerning alleged other critical infrastructure information. Specifically, Frontier argues that the Commission should further redact the Central Office identity information from Table 10.1, "as it would be possible for a third party to determine which Central Offices do not have diverse connections based on their omission from Table 10.2, particularly since other sections of the Network Report identify all of Frontier's Central Offices and the PD finds that Central Office information is publicly available."[273] Frontier similarly argues that Table 10.3 should be fully redacted or in the alternative, merely note the overall number of diverse and non-diverse connections. While we disagree with Frontier that

[273] Frontier Comments, at 14.

further redactions of these tables are necessary, we provide further explanation regarding this issue in the relevant discussion sections in the decision.

AT&T's and Frontier's joint reply comments reiterate that they do not oppose the proposed decision's disposition of the confidentiality status of the information at issue. They argue, however, that the proposed decision's interpretation of the applicable trade secret standards was incorrect and that modifications are necessary to avoid confusion regarding the applicable standards in future situations and to avoid creating precedent here which would deny the Commission flexibility to address confidentiality claims going forward. We disagree with the carriers' contention that our analysis of the applicable trade secret laws as applied to the information contained in the Network Report was incorrect. We do believe that further clarification of our analysis would serve to avoid confusion and therefore we have modified the decision accordingly to make clear that it was based on the specific facts and balancing of interests at stake here. No changes to the decision, other than those that clarify our position regarding the applicable trade secret standards, were made in response to comments.

9. Assignment of Proceeding

Commissioner Clifford Rechtschaffen is the assigned Commissioner and Karl J. Bemesderfer is the assigned Administrative Law Judge in this proceeding.

Findings of Fact

1. The Commission has broad authority, and extensive responsibility, for regulating telecommunications providers to ensure Californians receive high quality and reliable service.
2. The Commission favors open and transparent proceedings.

3. When the Commission chooses to permit information to be filed under seal or otherwise treated as confidential, it routinely limits the duration of the confidentiality period.

4. D.13-02-023, affirmed in D.15-08-041, ordered a study examining the telecommunications network infrastructure, facilities, policies, and practices of California's two largest ILECs, AT&T and Frontier ("Network Study"), based on these carriers' consistent failure to comply with General Order 66-C service quality standards.

5. The Commission recognizes the importance of safe and reliable utility systems and carrier networks, and this recognition was a substantial impetus for this current Network Study.

6. The results of the Network Study are detailed in an April 2019 report entitled "Examination of the Local Telecommunications Networks and Related Policies and Practices of AT&T California and Frontier California – Study conducted pursuant to the California PUC Service Quality Rulemaking 11-12-001, Decision 13-02-023, and Decision 15-08-041" ("Network Report").

7. The Network Study provides empirical data on the condition of network infrastructure, carrier infrastructure policies and procedures, the quality of existing communications services, and potentially informs the development of new and improved metrics to measure service quality.

8. The Network Study of network infrastructure and operations helps to identify vulnerabilities and potential problems so they can be addressed before actual failures occur.

9. The Network Study was performed by an independent consultant, Economics and Technology, Inc. (ETI), hired by the Commission.

10. The Commission's Communications Division oversaw ETI in its performance of the Network Study.

11. In producing the Network Report, ETI relied upon eight categories of information, described in this decision as Category 1 through 8.

12. Categories 1 through 4 consist of information AT&T and Frontier provided with accompanying claims of confidentiality.

13. Categories 5 through 8 consist of information obtained from public sources.

14. Category 1 information consists of reports and underlying raw data that AT&T, Verizon (prior to the transfer of its California ILEC operations to Frontier on April 1, 2016), and Frontier were required to provide to the CPUC on an ongoing basis pursuant to General Order 133-C/D regarding customer trouble reports and the respective companies' responses thereto. The Network Report includes this information in Chapters 2, 4, 4A, and 4F.

15. Category 2 information consists of AT&T and Frontier responses to data requests submitted by ETI and by CPUC Communications Division staff.

16. Category 3 information consists of information and photographs CPUC staff obtained from site visits (e.g., outage locations; network facility maps; photographs of equipment inside AT&T and Frontier Central Offices) conducted as part of the Network Study.

17. Category 4 information consists of annual financial reports AT&T California, Verizon California, and Frontier California file with the CPUC that conform to the FCC's ARMIS reporting requirements. While largely discontinued by the FCC after 2007, the CPUC has continued to require these reports to be filed by ILECs.

18. Category 5 information consists of public financial data and disclosures obtained from annual, quarterly and special reports – 10-K, 10-Q and 8-K reports – as filed by the two ILECs' parent companies – AT&T Inc., Verizon Communications, Inc. and Frontier Communications, Inc. – with the SEC, as well as Annual Reports to Shareholders and other shareholder communications issued by the various parent companies.

19. Category 6 information consists of industry data and reports the CPUC and the FCC publish.

20. Category 7 information consists of statewide and county-wide industry data for California the FCC publishes.

21. Category 8 information consists of information from government data sources, including the US Census Bureau, the Bureau of Labor Statistics, various California state agencies, and the National Oceanographic and Atmospheric Administration.

22. Much of the information provided by the carriers that is included in the Network Report is used for narrative purposes or for background in developing charts.

23. The Network Study covered an 8-year period of the carriers' operations, from 2010 through 2017.

24. The latest utility information summarized or otherwise referenced in the Network Report is from 2017.

25. CPUC Legal staff reviewed the carriers' confidentiality declarations and had concluded that, because of the general nature of the objections raised, these declarations did not adequately set forth the legal and factual grounds for confidential treatment of such information, as required in General Order 66-D.

26. The August 16, 2019 ACR directed the carriers to provide specific legal and factual bases for confidential treatment of any Network Study information provided to the Commission and ETI.

27. The August 16, 2019 ACR put the carriers on notice that a failure to make the requisite showing to justify confidential treatment of information would result in the disclosure of such information.

28. The Network Report does not include customer specific information such as customer identities, addresses, telephone numbers, contact information, type of service received from carriers, and similar personal information.

29. The out of service information summarized in the Network Report does not identify specific carrier equipment or facilities involved in individual outages or describe the specific causes of individual outages.

30. AT&T and Frontier claim all the raw data submitted pursuant to GO 133-D, §§ 3.3(d) and 3.4(d) warrants confidential treatment.

31. The Network Report aggregates and summarizes the "raw data" but does not include specific data concerning individual customer trouble reports or utility responses to such reports.

32. The Network Report aggregates this data for each of the carriers' wire centers in order to rank each wire center's performance with GO 133-C/D's Trouble Reports and Out-of-Service measures.

33. Raw trouble reports are based on information from customers who have called a carrier to complain about service issues.

34. Trouble reports contain information relayed to the carriers from their customers.

35. The Network Report includes tables summarizing trouble report and out-of-service statistics on an exchange or wire center by wire center basis, and on a number of trouble reports per 100 service line basis.

36. The GO 133-D service quality reporting requirements were developed by the Commission to obtain from carriers service quality data concerning five specific measurements (installation intervals, installation commitments, customer trouble reports, out-of-service repair interval, and operator answer time) to provide customers with information on how carriers perform; the reporting requirements, and the reported service quality measurements, were not developed or obtained independently by carriers.

37. The Commission does not routinely summarize and post raw GO 133-D trouble reports and out-of-service data on a monthly, wire center location-specific basis.

38. Customer complaint information obtained from a compilation of individual trouble tickets provides the public with important utility service quality and public safety information.

39. Out-of-service information associated with trouble reports and carrier responses to such trouble reports can be helpful in understanding what factors affect network reliability.

40. Restrictions on public access to relevant information impair the ability of parties and the public to participate effectively in Commission proceedings.

41. GO 133-D reports submitted to the Commission are not confidential.

42. AT&T and Frontier have access to GO 133-D service quality reports submitted by any Commission-regulated competitors and posted on the Commission's website.

43. AT&T and Frontier did not identify the economic value derived from non-disclosure of the raw data in the Network Report other than the speculative value of keeping largely negative service quality information hidden from potential competitors.

44. Disclosure of the trouble reports and out of service information discussed and summarized in the Network Report does not pose a threat to the security of carrier facilities or the public.

45. Disclosure of the out of service information discussed and summarized in the Network Report would enable parties to participate effectively in this proceeding, inform the public about network issues related to the extent to which Frontier and AT&T provide, or fail to provide, high quality safe and reliable network services, and permit the Commission to conduct this proceeding in an appropriately open and transparent manner.

46. Disclosure of the infrastructure and investment information discussed and summarized in the Network Report would enable parties to participate effectively in this proceeding, inform the public about network issues related to the extent to which Frontier and AT&T provide, or fail to provide, high quality safe and reliable network services in rural and urban locations, and permit the Commission to conduct this proceeding in an appropriately open and transparent manner.

47. With few exceptions, disclosure of the infrastructure information in the Network Report poses a purely speculative threat to the safety of network facilities or the public.

48. Some information regarding the physical network should not be revealed because doing so would pose a national security and/or public safety risk.

49. Many internet sites provide information regarding the locations of central offices, the common language locator codes associated with central offices, the types of switches installed at central offices, the identities of exchanges served by central offices, the types of broadband and other services available through central offices, and other details regarding telecommunications networks.

50. The marketing portions of the websites of AT&T and Frontier allow potential customers to identify the types of service they provide at specific locations.

51. The interactive broadband map available on the Commission's website provides a wealth of detail regarding the availability, type, and speed of broadband service at various locations in California, including locations served by Frontier and AT&T.

52. ARMIS Report and data request responses containing financial and infrastructure information on a USOA account by account basis include information in formats developed and mandated by regulatory agencies, specifically, the FCC, and the CPUC.

Conclusions of Law

1. The California Constitution Article 1, §§ 3(b)(1) and (2) favors disclosure of government records.

2. Gov. Code § 6255(a) provides that state agencies that wish to withhold public records from the public must base such withholding on express provisions of the CPRA or upon a demonstration that on the facts of the particular case the public interest served by withholding the records clearly outweighs the public interest served by disclosure.

3. The fact that a record may fall within a CPRA exemption does not preclude its disclosure.

4. CPRA exemptions are permissive rather than mandatory; they allow nondisclosure but do not prohibit disclosure.

5. Gov. Code § 6253.3 provides that the Commission cannot delegate to regulated entities, or others, the responsibility for making disclosure determinations.

6. Gov. Code § 6260 provides that CPRA exemptions cannot be asserted as a basis for withholding information in response to discovery.

7. Restrictions on public access to relevant information should not impair the ability of parties and the public to participate effectively in Commission proceedings and/or understand the activities of regulated entities and the Commission.

8. Gov. Code § 6254 does not prevent an agency from disclosing records received in conducting the people's business unless disclosure is otherwise prohibited by law.

9. GO 133-D § 2.2 reporting levels were established to provide customers with information about carrier performance.

10. GO 133-D § 3 requires carriers to report the number of trouble reports received per 100 working lines on an exchange or wire center basis, whichever is smaller.

11. GO 133-C and GO 133-D, §§ 3.3(d) and 3.4(d), require AT&T and Frontier to submit underlying raw data to substantiate the monthly data reported in the quarterly service quality reports.

12. GO 133-D § 4 requires carriers to report out of service repair intervals on a statewide basis and to provide underlying data on an exchange or wire center basis, whichever is smaller.

13. Disclosure of carrier performance information based on the aggregated monthly data of raw trouble reports by wire center and trouble reports per 100-working-lines is consistent with both GO 133-D and the Commission's general policies regarding the disclosure of complaint information.

14. It is reasonable for the Commission to treat different carriers differently if those carriers behave substantially differently from other members of the class of carriers, such as in this case, where Frontier and AT&T have failed to meet the service quality standards set forth by the Commission in GO 133-D.

15. Infrastructure and operational information that is available to the public is not a trade secret.

16. Information extracted from ARMIS reports submitted to the Commission, and used in the Network Report, is not the trade secrets of the carriers that submit them.

17. Service Quality Reports and the underlying raw data aggregated at the level disclosed in the Network Report, which have been submitted to the Commission as required by GO 133-D are not the trade secrets of the carriers who submit them.

18. Frontier failed to show that its Gov. Code § 6255(a) balancing test claims regarding the effect of disclosure on its competitive position are based on interests other than its private economic interests, which alone do not provide convincing evidence that the public would be harmed by disclosure.

19. Frontier failed to show that its Gov. Code § 6255(a) balancing test claims regarding the effect of disclosure on the competitive market for telecommunications services are primarily based on interests other than its private economic interests, which alone do not provide convincing evidence that

the operation of the competitive market would be harmed by disclosure in the Network Report, and that the public would be harmed as a consequence.

20. The Gov. Code § 6254(c) exemption is inapplicable to the customer data in the Network Report.

21. The Gov. Code § 6254(e) exemption for geological and geophysical data, plant production data, and similar information is inapplicable to information in the Network Report.

22. If information submitted to the Commission is subject to a statutory prohibition against disclosure, or to an applicable and properly asserted privilege, the Commission may withhold such information from responses to CPRA requests.

23. Evid. Code § 1060 provides that the owner of a trade secret has a privilege to refuse to disclose the secret, and to prevent another from disclosing it, unless asserting the privilege will tend to conceal fraud or otherwise work injustice.

24. A state agency's decision whether to disclose public records subject to trade secret privilege assertions requires a two stage analysis; first, the agency must determine whether the records include trade secrets; second, the agency must engage in a balancing of public interests for and against disclosure.

25. Information that is generally known to the public, or to portions of the public who can use the information for their economic benefit, is not a trade secret.

26. The underlying aggregated raw service quality data that carriers submit with the GO 133-D service quality quarterly reports, which are summarized in the Network Report, are not carrier trade secrets.

27. Generally, if a trade secret owner discloses a trade secret to those who have no obligation to maintain, or interest in maintaining, the secrecy of the trade secret, its legal protection is extinguished.

28. Information in the Network Report should not be withheld from the public on the basis of the trade secret privileges asserted by Frontier and AT&T.

29. The PCII Program (6 U.S.C. §671 et seq.) protects private sector infrastructure information voluntarily shared with the federal government for the purposes of homeland security.

30. Because the information in the Network Report was provided to the Commission rather than the federal government, the Commission is not bound by the requirements of the PCII Program under 6 U.S.C. § 673(a), as stated in 6 U.S.C. § 673(c).

31. The framework the Commission uses to analyze the carriers' claims regarding critical infrastructure is the CPRA balancing test, Gov. Code § 6255(a).

32. D. 17-09-023 and GO 66-D § 3.5 provide that the Commission will not treat information that is available to the public as confidential.

33. GO 133-D extends confidential treatment only to major service interruption reports required to be filed with the FCC and the Commission.

34. The Customer Trouble Reports and Out-of-Service Repair Interval raw data that is presented in the Network Report in the form of tables and charts summarizing monthly data by wire center are not subject to withholding by the Commission on the basis that the information would reveal the carriers' trade secrets.

35. The public interest served by disclosure to the public of those portions of the Network Report summarizing information from the service quality reports and raw data concerning trouble reports and out of service events clearly outweighs the public interest served by non-disclosure.

36. The public interest served by disclosing to the public portions of the Network Report summarizing financial and infrastructure information from the data request responses submitted to the Commission during the network examination, or summarizing information from the ARMIS reports submitted to the Commission and available to the Commission and ETS during the network examination, clearly outweigh the public interest served by non-disclosure, except to the limited extent set forth in this decision.

37. The Commission should not withhold from the public data request responses and ARMIS reports that include account-specific financial and infrastructure information based on the carriers' trade secret assertions.

38. Requests that the Commission withhold information from the public based on Gov. Code § 6255(a) must not be based solely on private economic interests.

39. Requests that the Commission withhold from the public information that is already public do not provide a lawful basis for withholding such information from the public.

40. Requests that the Commission withhold from the public information that is already public may represent a violation of GO 66-D and Rule 1.1 of the Commission's Rules of Practice and Procedure.

41. Mere assertions that disclosure of infrastructure information would endanger carrier facilities and the public are not sufficient to justify a finding that the public interest served by withholding records including infrastructure information clearly outweighs the public interest served by disclosure.

42. The public interest is served by the disclosure of almost all infrastructure information in the Network Report.

43. Redaction of a very limited amount of specific infrastructure information in the Network Report is in the public interest.

44. The public interest served by redacting the names and CLLI code numbers of the central offices from tables in the Network Report that identify the network diversity at specific central offices outweighs the public interest that would be served by disclosure.

45. Because much of the information provided by the carriers that is included in the Network Report is already public, there is no basis for nondisclosure of such information.

46. Balancing the public interest in nondisclosure with the public interest in disclosure, we find that for reasons of public safety, the following information provided by Frontier should not be disclosed at this time:

a. Detailed maps that contain information that is not typically made public, and which expose critical infrastructure that could make it easier for the network to be attacked.
b. Detailed maps of each Long Beach wire center.
c. The central office identity/location in tables showing diversity status.
d. The central office identity/location in tables showing PSAP connection diversity.
e. The central office identity/location in tables showing hours of backup power.

47. Balancing the public interest in nondisclosure with the public interest in disclosure, we find that for reasons of public safety, the following information provided by AT&T should not be disclosed at this time:

a. Maps showing the deployment of facilities by individual wire center and exchange maps for each wire center visited by CD staff.
b. The central office identity/location in tables showing central office diversity.
c. The central office identity/location in tables showing PSAP diversity.
d. The central office identity/location in tables showing hours of backup power.

48. Any security risk posed by the disclosure of investment and expense information for certain AT&T facilities does not outweigh the public interest in disclosure of such information.

O R D E R

IT IS ORDERED that:

1. The "Examination of the Local Telecommunications Networks and Related Policies and Practices of AT&T California and Frontier California – Study conducted pursuant to the California PUC Service Quality Rulemaking 11-12-001, Decision 13-02-023, and Decision 15-08-041" (Network Report), Chapters 3, 5, 6, 7, 8, 9, 10, and 12 shall be redacted by staff consistent with conclusions in this decision and shall be made available on the Commission's website within 30 days of the effective date of this decision.

2. The Network Report, Chapters 1, 2, 4, 11 and the Table of Contents shall be made available in their entirety on the Commission's website within 30 days of the effective date of this decision.

This order is effective today.

Dated December 17, 2020, at San Francisco, California.

MARYBEL BATJER
President
LIANE M. RANDOLPH
MARTHA GUZMAN ACEVES
CLIFFORD RECHTSCHAFFEN
GENEVIEVE SHIROMA
Commissioners