HUNTON& WILLIAMS

AOPL Business Conference
Newport Beach, California
September 18, 2013

Pipeline Information and FOIA: What Should Be Protected and How[1]

I. Overview of FOIA

A. Public Right to Know Statute

The Freedom of Information Act (FOIA) was originally enacted in 1966 under President Johnson. *5 U.S.C. 552*, *et seq*. FOIA provides that any person has the right to obtain access to federal agency records, except to the extent that portions of those records are protected from public disclosure by one of nine statutory exemptions. Most federal agencies have their own FOIA regulations for implementing the statute. *See e.g.*, *49 C.F.R. Part 7* (DOT's FOIA regulations). Further, every state has its own version of FOIA that may be applicable for intrastate pipelines that are regulated by certified states. *See e.g., Tex. Code Ann. § 552.001 – 552.353.* While modeled after FOIA, state public records laws are not identical to FOIA nor are state court interpretations of similar language.

B. Exemptions

FOIA sets forth nine statutory exemptions to public disclosure. *5 U.S.C. 552(b)*. Several have practical application to the pipeline industry including:

1. Trade secrets and commercial or financial information that is privileged or confidential (*FOIA Exemption 4*);

2. Personnel, medical files, and similar files the disclosure of which would constitute an invasion of personal privacy (*FOIA Exemption 6*); and

3. Information that is part of an ongoing enforcement proceeding (*FOIA Exemption 7*).

C. Homeland Security Issues Related to FOIA

Congress and the Department of Homeland Security have recognized that pipelines represent an important part of the critical energy infrastructure in the U.S. As a result, both have taken steps to limit the public disclosure of certain pipeline information that has national security implications. *See e.g.*, *5 U.S.C. 552(b)(3)* (FOIA Exemption 3 protecting information from disclosure that is otherwise protected by statute); *6 U.S.C. 133* (Critical Information Infrastructure Act of 2002); *6 U.S.C. 1207-1208* (implementing the recommendations of the 9/11 Commission). PHMSA has also taken steps to address the national security implications of making pipeline information public and to protect critical pipeline facilities. *See e.g., RSPA Pipeline Security Information Circular: Security Guidance for Natural Gas*

[1] As presented by Bob Hogfoss and Catherine Little, partners with Hunton & Williams LLP and leaders of the Firm's Pipeline Practice. For more information concerning Bob and Catherine, or their practice, visit www.pipelinelaw.com.

and Hazardous Liquid Pipelines and LNG Facilities (Sept. 5, 2002); *Annex to MOU between DHS and DOT concerning TSA and PHMSA Cooperation* (Aug. 6, 2006). While certain sensitive pipeline data shared with federal agencies may not fit squarely under various statutes and regulations that protect sensitive information from public disclosure, it likely falls within the type of data that Congress intended to protect and may arguably warrant protection for that reason.

II. FOIA Issues Affecting the Pipeline Industry

A. Facility Response Plans

Operators of onshore oil pipelines that due to their location could reasonably be expected to cause 'substantial harm,' or 'significant and substantial harm to the environment' by discharging oil to waters of the U.S. must prepare and submit a Facility response Plan (FRP) to PHMSA. *49 C.F.R. Part 194*; *see also 49 C.F.R. 194.121* (requiring that the plans be reviewed and revised every 5 years). FRPs contain sensitive information with regard to the anticipated consequences of an oil spill, including a worst case discharge, the maximum release time, the maximum shutdown response time, and the response resources available for responding to a release. Amendments to the Pipeline Safety Act in 2012 require PHMSA to maintain copies of FRPs and make those plans available to the public (although FOIA exemptions still apply). *49 U.S.C. 60138*. Unlimited access to these detailed plans may make pipeline infrastructure more vulnerable to attacks from potential terrorists.

B. In Line Inspection (ILI) Data

As part of integrity management requirements, operators perform ILIs to assess the integrity of their pipelines. *See 49 C.F.R. Part 195.45*2. ILI data contains detailed information regarding the internal conditions of oil and gas pipelines, and enables operators to identify the precise location of pipeline vulnerabilities. Operators are required to take corrective action in response to this data, but they are not required to submit the data to PHMSA or any other federal agency (PHMSA inspects the data during routine audits). Due to the sensitive nature of this information, pipeline operators typically keep ILI data confidential, although PHMSA may request the data in response to an incident or other investigation. General availability of ILI data, which identifies the type and precise location of anomalies (vulnerability), could be used by bad actors in planning damage to infrastructure, property or the environment. For this reason, there is a strong policy reason to protect ILI data from public disclosure.

C. SCADA and Control Room Information

Operators of pipeline facilities with a control room used to monitor and control the facility through a supervisory control and data acquisition (SCADA) system must adhere to PHMSA control room management regulations. *49 C.F.R. 195.446*. This includes developing detailed procedures and associated documentation to implement PHMSA requirements, submission of which may be required by the Agency (or certified states) in order to validate compliance. *49 C.F.R. 195.446(i)*. Infiltration of an operator's SCADA system by bad actors would allow access to and possible manipulation of real time information regarding the operational conditions of the pipeline, including pipeline leaks, safety alarms, and operation of valves used to shutdown segments of a pipeline.

D. Personnel Information

Numerous documents created or maintained by pipeline operators may contain employee names and personal information that is protected from disclosure under FOIA if disclosure would constitute an unwarranted invasion of personal privacy (*e.g.*, accident reports, investigation reports, etc.).

III. Options for Protecting Sensitive Information

A. Invoking Exemptions

1. Clear and Persuasive Facts Subject to Exemption

Information submitted to a federal agency may, either in whole or in part, clearly fall within an established FOIA exemption (*i.e.*, trade secret, financial information, enforcement confidential or other confidential information) or violate the principles of a FOIA exemption (*i.e.*, statutorily protected information with clear security implications). We recommend that all operators proactively mark information that may potentially be protected from disclosure under FOIA as "Confidential Information Protected from Public Disclosure" when making a submission to a federal agency.

2. Case-by-Case Approach

If the documents marked as confidential and protected from disclosure become the subject of a FOIA request, the federal agency should consult with the operator prior to making the decision whether to disclose the documents. While certain pipeline data shared with federal agencies may not fit squarely under various statutes and regulations that protect sensitive information from public disclosure, it likely falls within the type of data that Congress intended to protect and may arguably warrant protection for that reason. In determining whether to disclose documents to third parties, the Agency will consider the objections raised by an operator on a case by case basis.

B. Negotiated Resolutions

1. Redactions

In order to maintain control over redactions to protected portions of documents that are submitted to a federal agency, it may be beneficial to submit proposed redactions of any qualifying confidential information prior to submission. Many federal agencies have regulations regarding redacting documents that should be considered. *See e.g., 49 C.F.R. Part 190.209(d)* (requiring an operator who seeks confidential treatment of documents submitted in response to an enforcement action to submit a separate copy of the redactions with an explanation for each).

2. Restricted Access Agreements

An operator may also request the federal agency to sign an agreement regarding protected information to restrict copying and dissemination of the document and place appropriate other limitations, including return of the document or destruction.

3. Use of Limited Access Online Portals

Another option for limiting agency access to protected information could include providing temporary restricted access through internet websites or online portals.

C. Judicial Review ("reverse FOIA)" Challenges

If an agency makes a final determination to release information requested under FOIA, operators seeking to prevent the agency from disclosing that information to a third party may file what is referred to as a

'reverse FOIA' action under the Administrative Procedure Act (APA). The reviewing court will apply the arbitrary and capricious standard of judicial review based on the agency's administrative record. The challenge to disclosure will be reviewed in light of the statute's purpose to provide public access to agency documents and the FOIA exemptions which are to be construed narrowly.

1. Confidential Information

For purpose of FOIA Exemption 4, the D.C. Circuit narrowly interprets what may be considered a trade secret protected from disclosure under FOIA. *Public Citizen Health Research Group v. FDA, 704 F.2d 1280, 1288 (D.C. Cir. 1983)* (defining a trade secret as a "secret commercially valuable plan…process or device that is used for the making, preparing…or processing of trade commodities and [is] the end product of either innovation or substantial effort.").

With respect to commercial or financial information under FOIA Exemption 4, courts interpret those terms broadly. *See e.g.*, *Critical Mass Energy Project v. NRC, 830 F.2d 278, 281 (D.C. Cir. 1987)*. The more difficult hurdle is establishing that the information is 'confidential.' Established case law under FOIA Exemption 4 distinguishes between confidential information that is mandatory versus voluntarily submitted information, requiring a higher threshold to establish exemption for information that is compelled by an agency. *National Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974)* (mandatory submission); *Critical Mass, 830 F.2d 278 (D.C. Cir. 1987)* (voluntarily submitted). Voluntarily submitted information is typically given more protection from disclosure. Where information is required to be submitted to an agency, it can still be maintained as 'confidential' if disclosure is likely to either (1) impair the government's ability to obtain the information in the future; or (2) cause substantial competitive harm to the person who submitted the information. *National Parks, 498 F.2d 765, at 770.*

Unexercised agency authority, or "the mere power to compel" certain submissions, does not constitute a requirement to make submission, and thus any information that is submitted to an agency absent a pre-existing requirement to do so should be considered voluntary. *See U.S. Department of Justice FOIA Update*, Vol. XIV, No. 2, at 3-5; *("OIP Guidance: The Critical Mass Distinction under Exemption 4")*. Information voluntarily provided to the government is considered 'confidential' under a lower threshold, "if it is of a kind that the provider would not customarily release to the public." *Critical Mass, 975 F.2d 871, at 880.*

2. Personnel Information

To warrant protection of personnel information under FOIA Exemption 6, the information must (1) consist of "personnel and medical files and similar files;" and (2) disclosure of the information would "constitute a clearly unwarranted invasion of personal privacy." *5 U.S.C. 552(b)(6)*. The Supreme Court has broadly construed the type of information protected from disclosure, making clear that all information that "applies to a particular individual" meets the threshold requirement for Exemption 6 protection. *U.S. Dep't of State v. WA. Post Co., 456 U.S. 595, 602 (1982); see also N.Y. Times Co. v. NASA, 920 F.2d 1002, 1005 (D.C. Cir. 1990) (en banc)* (extending application to tape recordings because voices contain personal information).

Assuming the information meets the first requirement of FOIA Exemption 6, the focus of the inquiry turns to whether disclosure of the records at issue "would constitute a clearly unwarranted invasion of personal privacy." Information submitted to a governmental agency that contains personal information of employees (names, addresses and other contact information that is not widely available to the public, etc.) should be prohibited from disclosure to the public under Exemption 6 of FOIA because of the personal

nature of that information. *See Sherman v. U.S. Dep't of the Army, 244 F.3d 357, 363-64 (5th Cir. 2001)*.

If a privacy right exists to the information, then the public interest in disclosure must be weighed against the privacy interest in nondisclosure. *U.S. Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989)*. If no public interest exists, the information should be protected.

3. Enforcement Proceedings

FOIA Exemption 7 protects records or information compiled for law enforcement purposes. In order for the exemption to apply, it must be shown that production of the information: (1) could reasonably be expected to interfere with enforcement proceedings; (2) would deprive a person of a right to a fair trial or an impartial adjudication; (3) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (4) could reasonably be expected to disclose the identity of a confidential source; (5) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions; or (6) could reasonably be expected to endanger the life or physical safety of any individual. *5 U.S.C. 552(b)(7).* The Supreme Court has held that information not initially obtained or generated for law enforcement purposes may still qualify under Exemption 7 if it is subsequently used for a law enforcement purpose at any time prior to "when the Government invokes the Exemption." *John Doe Agency v. John Doe Corp., 493 U.S. 146, 153 (1989)*.

Exemption 7 applies equally to records compiled to enforce state or federal law, which includes both civil, criminal, and administrative proceedings statutes. *See Hopkinson v. Shillinger, 866 F.2d 1185, 1222 n.27 (10th Cir. 1989); Jefferson v. DOJ, 284 F.3d 172, 178 (D.C. Cir. 2002)*. In addition, there is no requirement that the matter result in actual administrative, civil, or criminal enforcement. *See Pratt v. Webster, 673 F.2d 408, 420-21 (D.C. Cir. 1982).* To establish its threshold burden to satisfy Exemption 7 and withhold documents from disclosure, an agency is not required to identify a particular individual or incident as the object of investigation, it must merely "demonstrate a relationship between its authority . . . and the activity giving rise to the requested documents . . . supports at least a colorable claim of the relationship's rationality." *Abdelfattah v. DHS, 488 F. 3d. 178, 185 (3d. Cir. 2007).*

D. Request for Rulemaking or Legislation rulemaking

PHMSA has not yet refined its FOIA or related Homeland Security regulations or procedures, leaving both the Agency and the industry vulnerable to FOIA challenges. The industry may want to consider a Petition for Rulemaking or even legislative change to effect change to the Agency's FOIA practices in order to ensure better protections for sensitive information as well as consistency in application. More detailed FOIA regulations and procedures could afford more reliable protection of confidential, sensitive security and private personal information.