

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF OHIO  
EASTERN DIVISION

IN RE: NATIONAL PRESCRIPTION )  
OPIATE LITIGATION )  
)  
)  
)  
)  
)  
)  
)

CASE NO. 1:17-MD-2804  
JUDGE DAN A. POLSTER  
MAGISTRATE JUDGE DAVID A. RUIZ

---

**UNITED STATES OF AMERICA'S  
BRIEF IN SUPPORT OF OBJECTIONS TO DISCLOSURE OF ARCOS DATA**

---

DAVID A. SIERLEJA  
First Assistant United States Attorney  
Northern District of Ohio  
JAMES R. BENNETT II (OH #0071663)  
KAREN E. SWANSON HAAN (OH #0082518)  
Assistant U.S. Attorneys  
Carl B. Stokes United States Courthouse  
801 West Superior Avenue, Suite 400  
Cleveland, Ohio 44113-1852  
(216) 622-3988 (Bennett)  
(216) 622-3851 (Swanson Haan)  
E-mail: James.Bennett4@usdoj.gov  
E-mail: Karen.Swanson.Haan@usdoj.gov

ALEXANDER K. HAAS  
Special Counsel to the Assistant AG, Civil Division  
ALICE SHIH LACOUR  
ERIC J. SOSKIN  
Counsel to the Assistant AG, Civil Division  
United States Department of Justice  
950 Pennsylvania Ave., NW  
Washington, DC 20530  
(202) 353-8679 (Haas)  
(202) 514-3180 (LaCour)  
(202) 514-1500 (Soskin)  
E-mail: alex.haas@usdoj.gov  
E-mail: alice.s.lacour@usdoj.gov  
E-mail: eric.soskin@usdoj.gov

## **I. PRELIMINARY STATEMENT**

In this Multidistrict Litigation (“MDL”), public entities from across the nation have sued manufacturers, distributors and retailers of prescription opiate drugs, alleging that they are liable for the opioid public health crisis. To assist the Court and the parties in addressing the crisis, the Drug Enforcement Administration (“DEA”) and the Department of Justice (“DOJ”) (collectively “United States”) produced transactional data for all 50 states and several territories from its Automation of Reports and Consolidated Orders System (“ARCOS”) database. Because the data contains law enforcement sensitive and Privacy Act protected information, and is treated as confidential business records and trade secrets by the reporting companies, DEA does not release ARCOS data publicly and only produced it here under the safeguards of the Protective Order.

Recipients of the data have received Public Records Requests for the data from the media (“Requesters”). (ECF Nos. 603-1, 603-2, 603-3.) However, the Protective Order limits the use of the data “(1) to mediate, settle, prosecute, or defend the...litigation, or (2) for law enforcement purposes.” It does not authorize disclosure to Requestors. Because there is substantial risk that release of the data would invalidate this Court’s protections, undermine the United States’ ability to combat the opioid crisis, undercut DEA’s investigatory and enforcement actions, violate the privacy and trade secret rights of third-parties, and facilitate criminal activity, the United States opposes release of the data to Requestors.

## **II. FACTS AND PROCEDURAL HISTORY**

### **A. DEA’s ARCOS Database**

Pursuant to 21 U.S.C. § 827(d)(1), registrants must report to DEA “every sale, delivery or other disposal by him of any controlled substance....” DEA maintains a database of these transactions in ARCOS—an automated, comprehensive drug reporting system of records that monitors the flow of controlled substances from their point of manufacture through commercial

distribution channels to the point of sale or distribution at the retail level. (*See* Declaration of Assistant Administrator for Diversion Control, DEA, John J. Martin (“Martin Decl.”) at ¶ 6.) The data contained in ARCOS includes the supplier name, registration number, address, and business activity; buyer name, registration number, and address; and drug code, transaction date, total dosage units, and total grams. (*Id.* at ¶ 7.) Approximately 1,200 manufacturers and distributors are required by law to report to ARCOS. (*Id.*)

**B. Law Enforcement Uses**

DEA is authorized to enforce the Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. § 801, *et seq.*, by investigating trafficking in controlled substances; seizing and forfeiting assets related to illicit drug trafficking; and cooperating with counterpart agencies. DEA relies on ARCOS in its regulatory and law enforcement missions. DEA does not make ARCOS data generally available to the public. Rather, it uses ARCOS, among other things, to: (a) identify patterns and trends in the flow of all Schedule I, II controlled substances; and Schedule III narcotic controlled substances under the Controlled Substances Act (“CSA”); (b) review and verify specific registrant activities and registrant self-reporting accuracy to assist diversion investigators with accountability audits during scheduled onsite regulatory investigations; and (c) provide field diversion investigators with tips, leads, and pointers of potential diversion of pharmaceutical controlled substances. (Martin Decl. at ¶ 9.)

DEA provides ARCOS data to investigators in federal, state and local government agencies throughout the United States on a case by case basis to identify and combat the diversion of controlled substances into illicit channels of distribution. (*Id.* at ¶ 10.) U.S. Attorneys and DEA investigators also use the information to strengthen criminal cases.

**C. Friend of the Court**

Though not a party to the MDL, the United States sought permission to participate in settlement discussions and as a friend of the Court. (ECF No. 212, PageID # 1032.) As such, the United States agreed to provide information to facilitate effective non-monetary remedies. In that role, and consistent with the Court's orders, the United States provided nine years of ARCOS transactional data spanning January 1, 2006 to December 31, 2014 for all 50 states and several U.S. territories. DEA made this production subject to the Protective Order and solely for use in the MDL litigation and law enforcement efforts across the country.<sup>1</sup> However, the data remains the property of the United States and was never intended for public dissemination.

**D. The Court's Protective Order**

When plaintiffs first sought ARCOS data, DEA expressed concerns about wholesale production of the data. In particular, DEA feared that the plaintiffs, most of whom are public entities, would be obligated to publicly disclose DEA's data pursuant to public records requests. Because the ARCOS data contains law enforcement sensitive and Privacy Act information, and is treated as trade secrets and confidential business records, public disclosure of the data would undermine the United States' efforts to combat the opioid crisis, violate the privacy and trade secret rights of third-parties, and facilitate criminal activity.

The Court acknowledged the United States' concerns about making the data public and stated that the ARCOS data is "not going to be public, so there will be a protective order." (Hearing Tr. at 13.) The Court entered a Protective Order providing that disclosure of the data would be "to the governmental plaintiffs . . . and . . . to State Attorneys General for litigation and law

---

<sup>1</sup> To the extent that DEA may make future ARCOS productions, the arguments made herein apply equally to any future public records requests for such data.

enforcement purposes.” (ECF No. 167 PageID # 937.) The Protective Order authorized the use of ARCOS data for only two purposes: “(1) to mediate, settle, prosecute, or defend the... litigation, or (2) for law enforcement purposes.” (ECF No. 167 at PageID # 939.) It also limited distribution to the following authorized individuals: employees and agents of counsel, court reporters, the judge and his staff, experts, and state and local law enforcement. (*Id.* at PageID # 940.)

#### **E. Public Record Requests Received by Plaintiffs**

On June 8, 2018, the United States received notice of three public records requests from the media seeking disclosure of the ARCOS data produced in the MDL. (Notice of Objections, ECF No. 603, PageID # 14958.)<sup>2</sup> On June 11, 2018, the United States objected to disclosure of the data. (Notice of Objections, ECF No. 603, PageID # 14958; *see also*, ECF No. 167 PageID #942.) On June 13, 2018, the Court issued an order “suspend[ing] the obligation of DEA or Defendants to file objections to [additional Public Records Requests]...” and ordered briefing. (Order ECF No. 611, PageID # 14995.) Since that time, the United States has received notice of additional requests and likewise opposes disclosure of ARCOS data in response to those requests.

### **III. LEGAL ARGUMENT**

#### **A. Disclosure of the ARCOS Data Would Violate the Court’s Protective Order**

As noted above, the Court has acknowledged that a protective order is necessary to shield the ARCOS data from public dissemination. (Hearing Tr. at 13.) Accordingly, the Court significantly limited the permissible uses of the data and issued a narrowly-tailored protective order providing that the data “shall remain confidential and shall be used only for litigation

---

<sup>2</sup> The first was an Open Records Law Request to the County of Cuyahoga, Ohio by the Washington Post in a letter dated June 7, 2018. (ECF No. 603-1, PageID # 14962.) The second was an Open Records Law Request to the County of Summit, Ohio by the Washington Post in a letter dated June 7, 2018. (ECF No. 603-2, PageID # 14964.) The third was a West Virginia Freedom of Information Act Request to the Cabell County Commission, West Virginia by HD Media Company, LLC in a letter dated June 5, 2018. (ECF No. 603-3, PageID # 14966.)

purposes or in connection with state and local law enforcement efforts.” (ECF No. 167 at PageID # 937; *see also id.* at PageID # 939 (listing limited authorized uses). The Court also specified that the data “shall not be used by any person or entity for commercial purposes, in furtherance of business objectives, or to gain a competitive advantage.” (*Id.*)

Disclosure of the ARCOS data here should be denied because it is not among the authorized uses of the data under the Protective Order. None of the Requestors are parties to the litigation or law enforcement entities and there is no suggestion that they intend to use the data for any of the authorized purposes. Therefore, the Protective Order does not permit disclosure to them. Indeed, to the extent the Requestors would use the data for commercial purposes or in furtherance of their business objectives, such use is expressly prohibited. (ECF No. 167 at PageID # 939.)

Moreover, allowing the ARCOS data to be disclosed pursuant to public records requests would eviscerate this Court’s Protective Order and contradict the bedrock principles that “[d]iscovery . . . is essentially a private process . . . the sole purpose of [which] is to assist trial preparation.” *United States v. Anderson*, 799 F.2d 1438, 1441 (11th Cir.1995). Courts have recognized “numerous pitfalls in allowing unfettered public access to discovery materials,” including by undermining “the purpose of the discovery rules—to encourage the disclosure of information and materials to avoid unnecessary surprise and to level the playing field.” *United States v. Smith*, 985 F. Supp. 2d 506, 520 (S.D. N.Y. 2013).

Once data is deemed a public record by any entity, there would be no limit on who could obtain the information and for which purposes it could be used. This would nullify the Protective Order and convert protected discovery in this proceeding into a massive release of the government’s ARCOS data for use by anyone for any purpose whatsoever. Other courts have rejected efforts to use state records laws to modify a federal court’s protective order. *See, e.g., United States v. Loughner*, 807 F. Supp. 2d 828, 834 (D.Ariz. 2011) (rejecting argument by news

organizations that federal protective order be modified to permit disclosure through public records requests made to state-agency investigative partners). Release to the public is inconsistent with the Court's previous authorization of discovery only pursuant to the narrow Protective Order.

**B. ARCOS Data is Federal Property Subject to the United States' Control.**

“Confidential business information has long been recognized as property.” *Carpenter v. United States*, 484 U.S. 19, 25 (1987) (newspaper column property under 18 U.S.C. § 641). In *Carpenter*, the Supreme Court considered whether information a Wall Street Journal writer obtained to prepare a financial column was property. The Court held that the intangible nature of the information did not make it any less property. “Confidential information acquired or compiled by a corporation in the course and conduct of its business is a species of property to which the corporation has the exclusive right and benefit, and which a court of equity will protect through the injunctive process or other appropriate remedy.” *Id.* at 26. The Court confirmed the well-established principle that even in the absence of a written contract, one who acquires special knowledge or information as a result of a confidential relationship with another must account to the principal for any use of the information. *Id.* at 27-28.

Because information is property, courts have recognized that, as a matter of federal common law, the United States has the authority to enforce its property interest in its records in the context of state public records requests. *See, e.g., United States v. Napper*, 694 F. Supp. 897 (N.D. Ga. 1988), *aff'd*, 887 F.2d 1528 (11th Cir. 1989) (enjoining the Atlanta from disclosing FBI investigative files in response to a state records request and holding that Atlanta had “no right to disseminate” the files, which it had received in confidence, because such files were federal property); *United States v. Story County, Iowa*, 28 F. Supp. 3d 861 (S.D. Iowa 2014) (enjoining the county from publicly releasing emails located on the county server that had been sent and received by a county sheriff in his capacity as a member of a federal board and finding that the

records were “federal records and not subject to Iowa’s Public Records Act.” *Id.* at 872); *United States v. City of Seattle*, Case No. 16-cv-889, 2017 WL 176541, at \*1 (W.D. Washington, Jan. 17, 2017) (enjoining Seattle from disclosing information that the FBI shared concerning pole camera locations and ruling that the information was “federal property, subject to the FBI’s right to control” such that it was protected by federal law from disclosure by the state public records law).

Here, the ARCOS data is the property of the United States. The right to control and disseminate the information is exclusive to the United States. The recipients lack the right to disclose the information pursuant to a public records request. The United States has sought to protect this highly sensitive information and provided it only pursuant to the Protective Order. Third-parties may not circumvent federal protections and attempt to acquire the data through a state entity or under state law. The correct forum is in federal court and under federal law. Thus, the recipients of the data do not have the right to disclose it and disclosure should be prohibited.

### **C. Disclosure would Undermine Law Enforcement Efforts**

The ARCOS database contains information that is law enforcement sensitive and its disclosure would undermine DEA’s ongoing and future law enforcement investigations, enforcement actions, or prosecutions. *See* Martin Decl. at ¶¶ 13-18, 27-37. Therefore, the data should be protected by the law enforcement investigatory privilege, “a qualified privilege designed to prevent disclosure of information that would be contrary to the public interest in the effective functioning of law enforcement.” *Tuite v. Henry*, 181 F.R.D. 175, 176 (D.D.C. 1998); *see also* *Friedman v. Bache Halsey Stuart Shields, Inc.*, 738 F.2d 1336, 1341 (D.C.Cir.1984) (“[t]here is surely such a thing as a qualified common law privilege ... for law enforcement investigatory files”). “The privilege serves to preserve the integrity of law enforcement techniques and confidential sources, protects witnesses and law enforcement personnel, safeguards the privacy of individuals under investigation, and prevents interference with investigations.” *Id.* at 176-77; *see*



also *Black v. Sheraton Corp. of America*, 564 F.2d 531, 542 (D.C.Cir.1977) (stating “law enforcement operations cannot be effective if conducted in full public view...” and recognizing the privilege under common law to allow for “pragmatic adjustment to the needs of sound government.”).

ARCOS data may suggest particular activities or patterns of activity that raise red flags about potential drug diversion that DEA will then investigate. *See* Martin Decl. at ¶¶ 13-14. After DEA conducts its investigation in reliance on the data, it further uses such data, together with the results of the investigation, to determine whether to bring an enforcement action. *Id.* at ¶ 15. Public disclosure of ARCOS data risks undermining active investigations that rely on ARCOS information. If the press were to receive access to the data, their efforts to interview an individual could tip off a potential target before DEA had the opportunity to investigate. Therefore, public disclosure of the data would be detrimental to DEA’s investigative efforts and could ultimately impede DEA’s efforts to bring enforcement actions. *Id.* at ¶ 16.

Importantly, “[a]n investigation...need not be ongoing for the law enforcement privilege to apply as ‘the ability of a law enforcement agency to conduct future investigations may be seriously impaired if certain information’ ” is revealed to the public. *Nat’l Congress for P.R. Rights ex rel. Perez v. City of N.Y.*, 194 F.R.D. 88, 95 (S.D.N.Y.2000) (quoting *Morrissey v. City of N.Y.*, 171 F.R.D. 85, 90 (S.D.N.Y.1997)); see also *Halpern v. FBI*, 181 F.3d 279, 294 (2d Cir.1999). Nor is the applicability of the law enforcement privilege dependent on whether the information was voluntarily provided to the government; investigations are equally subject to disruption regardless of the investigative means used to obtain information, and the willingness of those providing information to do so fulsomely may likewise be deterred even where the government compels production. *See Dellwood Farms v. Cargill*, 128 F.3d 1122, 1125 (7th Cir. 1997) (recognizing law

enforcement privilege protects the government from “being force[d] to tip its hand to criminal suspects and defendants by disclosing the fruits” of its activities).

The risk of adverse impact on DEA investigations and enforcement actions exists regardless of the age of the ARCOS data. Frequently, DEA investigations remain open for multiple years so that appropriate evidence can be gathered and DEA can assess the viability of a potential legal or enforcement action against the target. Therefore, it is not unusual for ARCOS data first generated a decade ago to continue to have relevance in ongoing investigations and enforcement actions. *See* Martin Decl. at ¶ 17. DEA currently has [REDACTED] open cases from 2006 to 2014 involving opioids. This includes multiple cases each year and progressively more cases in later years, culminating in [REDACTED] open cases in 2014. *Id.* at ¶ 27. *See also* Exhibit 1 to Martin Decl. Therefore, public disclosure of the ARCOS data could adversely impact DEA’s law enforcement efforts and administrative actions in [REDACTED] open cases from 2006 to 2014. *Id.* at ¶ 28.

[REDACTED]

[REDACTED] Martin Decl. at ¶¶ 29-30.

Despite being shared with the parties to this case, ARCOS information remains a DEA record. 44 U.S.C. § 3301(a)(1)(A) (a Federal record is any recorded information made or received by a Federal agency under Federal law). The disposition of a Federal record is a matter of Federal

law, not state law. *Id.* § 3102(2) (head of an agency must exercise effective control over the use of agency records) and 5 U.S. C. § 552 (The Freedom of Information Act (FOIA) exempts certain Federal records from public disclosure.) FOIA explicitly exempts from public disclosure records compiled for law enforcement purposes to the extent such disclosure could reasonably be expected to, *inter alia*, interfere with enforcement proceedings, deprive a person of a right to a fair trial or an impartial adjudication, or disclose law enforcement or prosecutorial techniques and procedures. 5 U.S.C. § 552(b)(7). This FOIA exemption protects ARCOS information from public disclosure. *See e.g., NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 236 (1978) (FOIA Exemption (b)(7) disclosure of investigatory records in pending case would interfere with enforcement proceedings).

The Sixth Circuit recently held that the FBI properly withheld information under the law-enforcement FOIA exemption. *ACLU of Mich. V. FBI*, 734 F.3d 460 (6th Cir. 2013) (finding that release of certain demographic data could have revealed law-enforcement priorities and methodologies, that the FBI provided reasonably segregated portions of the data, and that the requester’s initial proposal inadequately protected law-enforcement-sensitive information); *see also NAACP v. ACUSport, Inc.*, 271 F. Supp. 2d 435 (E.D.N.Y. 2003) (allowing limited disclosure of ATF’s Firearms Tracing System database in public nuisance lawsuit, but noting that “linking a traced gun to a specific crime location, as well as identifying data concerning the firearms distributor and dealer,” is law-enforcement-sensitive requiring strong protective order). Similarly, ARCOS data should be protected from state public record requests because it is law enforcement sensitive information and its disclosure would undermine law enforcement efforts.

**D. Disclosure of the ARCOS Data Would Contravene the Privacy Act.**

DEA’s authorization to operate ARCOS is subject to numerous privacy requirements. ARCOS is a Privacy Act System of Records. *See* 69 Federal Register 51104 and modified at 72 Federal Register 3410. Congress enacted the Privacy Act, 5 U.S.C. § 552a, “to protect against

invasion of an individual's personal privacy by . . . providing individuals with more control over the gathering, dissemination, and accuracy of [government] agency information about themselves." *Unger v. District Disclosure Office IRS*, 1:99-CV-698, 2000 U.S. Dist. LEXIS 16064, at \*5-6 (N.D. Ohio Sep. 18, 2000). The release of personally identifiable information from a federal system of records without the individual's consent violates the Privacy Act. *Id.*

Here, many of the ARCOS registrants are individuals, and the Privacy Act protects their information. None of them have consented to the disclosure of their information. Because disclosure of ARCOS data could reveal the name and DEA registration number of individual registrants, DEA is legally obligated to protect their legitimate privacy interests. Indeed, DEA could subject itself to private lawsuits by individuals whose data is improperly released outside its routine use. *See, e.g., Kinman v. United States*, No. 1:16-CV-329, 2016 U.S. Dist. LEXIS 169447, at \*10 (S.D. Ohio Dec. 7, 2016) (stating Privacy Act provides a private cause of action against federal agencies for violations); *see also* 5 U.S.C. § 552a(g)(1).

DEA provided ARCOS data when ordered to do so by the Court, subject to the Protective Order. 5 U.S.C § 552a(b)(11). To allow the recipients to make protected information available to the public usurps the purposes of the Privacy Act and invades the privacy of the individuals involved, most of whom are not parties to this litigation. Because of the privacy interests implicated, the Court should prohibit those receiving the data from making the data public.

Public disclosure of ARCOS data also could cause the media or others to incorrectly focus on an individual or company that has not done any wrong. Unlike DEA diversion investigators who work with ARCOS data regularly and are trained to interpret and understand patterns of activity, members of the public do not have such training. Without knowing how to interpret the ARCOS data, the media could unnecessarily bring attention to an individual or company that has done nothing wrong. *See Martin Decl.* at ¶¶ 32, 35.

**E. Disclosing ARCOS Would Reveal Confidential Commercial Information and Trade Secrets**

DEA is required to protect the trade secrets and commercial or financial information obtained from a registrant that is privileged or confidential. 21 U.S.C. § 830(c)(1). This includes records of regulated transactions such as sales, deliveries or disposals of any controlled substance. 21 U.S.C. § 830(a). Further, it is the policy of the United States—enforced by the threat of criminal sanction—to protect as confidential the business records commercial enterprises are compelled to give the government. *See* 18 U.S.C. § 1905 (stating that any federal employee who unlawfully discloses any information obtained in the course of his employment—including trade secrets and confidential commercial data—shall be fined or imprisoned or both, and shall be removed from federal employment.) Thus, the *Touhy* regulations prohibit the disclosure of official information that would reveal trade secrets without the owner’s consent. *See* 28 C.F.R. § 16.26(b)(5).

21 U.S.C. § 830(c)(1) incorporates FOIA’s exemption 4, which prohibits disclosure of trade secrets and confidential commercial information. 5 U.S.C. § 552(b)(4). Under FOIA exemption 4, data is “confidential commercial information” if “disclosure of the information is likely to: (1) impair the Government’s ability to obtain necessary information in the future or (2) cause substantial harm to the competitive position of the person from whom the information was obtained.” *Nat’l Parks & Conservation Ass’n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974) (explaining exemption may be invoked if public disclosure of commercial information is likely to cause substantial harm to competitive position). Federal courts have repeatedly recognized the government’s right to invoke FOIA exemption 4 in defense to a subpoena when the data was reported to the government and public disclosure would harm the competitive interests of the reporting party. *See, e.g., N.H. Right to Life v. United States HHS*, 778 F.3d 43 (1st Cir. 2015); *Am. Mgmt. Servs. V. Dep’t of the Army*, 703 F.3d 724 (4th Cir. 2013).

The ARCOS database contains over 80,000,000 transactions annually. None of the Registrants who provided ARCOS information to DEA have consented to its release. The data contained in ARCOS would establish a complete customer list including location and amount of sales. Disclosing the data could cause substantial competitive harm by giving entities information about their competitors' business strategies, market shares, and inventory levels. *See Madel v. U.S. Dep't of Justice*, 784 F.3d 448, 453 (8th Cir. 2015) (holding that disclosure of ARCOS information would "likely" cause "substantial competitive harm"). More importantly, the harm would impact not only on the litigants, but also numerous retail registrants who are not parties to this litigation and whose confidential transaction data would become public. Moreover, the consumers that rely on competition to control the costs of prescription medicines would be harmed. Thus, the data should not be released publicly.

**F. The ARCOS Data is Protected by the Required Report Privilege**

Federal courts have recognized that information a party submits to a government agency is protected from disclosure by a "required reports" privilege. *Ass'n for Women in Science v. Califano*, 566 F.2d 339 (D.C.Cir.1977); *In re Grand Jury Subpoena Dated November 14, 1989*, 728 F.Supp. 368 (W.D.Penn.1990). The privilege has two principal prerequisites. First, the report must be mandated. Second, federal law must provide for the privilege.

The registrants are mandated to report to DEA the information contained in the ARCOS database. 21 U.S.C. § 827(d)(1) (DEA registrants are required to report to DEA "every sale, delivery or other disposal by him of any controlled substance..."). Second, the data is confidential under 21 U.S.C. § 830(c)(1) ("any information obtained by the Attorney General under this section which is exempt from disclosure under section 552(a) of Title 5, by reason of section 552(b)(4) of such title, is confidential and may not be disclosed to any person."). Because the registrants are required to report their confidential commercial activity, the required report

privilege protects the information from public disclosure and those who have received the data should be prohibited from producing the data in response to public records requests.

### **G. Disclosure Would Facilitate Criminal Activity**

There is a substantial risk that making ARCOS data publically available will facilitate criminal activity. In the last ten years, the theft and loss of opioids has become a major problem. Disclosing ARCOS data would allow criminals to strategically plan robberies of controlled substances. Criminals would know the specific day a specific pharmacy receives large quantities of opioids and can plan their criminal activities accordingly. There are numerous recent examples of such robberies across the country. In Illinois and Indiana alone, police responded to more than 500 pharmacy robberies in those states between 2012 and 2017. In 2017, 11 defendants were sentenced based on federal pharmacy robbery indictments in Ohio. In April 2018, a pharmacy in Florida was robbed at gunpoint for cash and Oxycotin. That same month, a Walgreens pharmacy in Delaware was robbed of Oxycodone. In June 2018, two pharmacies were robbed of Oxycodone in Virginia within one week.<sup>3</sup>

If released publicly, ARCOS information could allow criminals to trace the flow of pills. Knowing where manufacturers and distributors are selling the most opioids would allow criminals to target those particular locations and attract more drug seekers to the area who are often associated with collateral crimes that adversely impact communities. Even if the addresses of

---

<sup>3</sup> <https://www.nbcchicago.com/investigations/Pharmacy-Robberies-a-Nasty-Side-Effect-of-Nations-Opioid-Crisis-422408144.html>; <https://www.justice.gov/usao-sdoh/pr/two-pharmacy-robbery-defendants-sentenced>; <https://www.floridatoday.com/story/news/crime/2018/04/26/melbourne-pharmacy-robbed-search-underway/553367002/>; <https://www.delawareonline.com/story/news/local/2018/04/20/lewes-pharmacy-robbery-police-chase/537895002/>; <http://www.wjhl.com/local/masked-suspect-in-bristol-va-pharmacy-robbery-passes-note-demanding-oxycodone-in-30-seconds-/1213492365>. Additional examples include: in 2017, a rash of armed pharmacy robberies in Ohio targeting Oxycodone <http://local12.com/news/local/harrison-police-search-for-the-two-robbers-who-held-up-a-pharmacy>; from 2016 to 2017, 40 Walgreens were robbed in Atlanta. <https://www.ajc.com/news/crime--law/pharmacy-robbed-pain-pills-separate-times/G9O89qLYDzq5cYwLW04trJ/>

certain warehouse locations and distribution centers are publicly available, this does not undercut the argument that ARCOS data should be protected. As the rising opioid thefts indicate, criminals are targeting locations where opioids are available. The existence of the location alone will not make it a target; which drug is there and in which quantity will increase the risk it will be targeted. Information about opioid quantities by location is not publicly available. That information, however, is available in ARCOS. If criminals are able to match a publicly available address with the quantities of opioids at that location from ARCOS, this increases the risk that such locations will be targeted. *See* Martin Decl. at ¶¶ 36-37.

The same is true at virtually every level of the distribution chain. For example, if criminals know which doctors are prescribing the most opioids, they can target those. One reason the Court issued the Protective Order was to restrict access of ARCOS data to a limited and defined scope of individuals, so as not to exacerbate the opioid crisis by increasing the likelihood that more opioids would reach the hands of the criminals. Allowing recipients of the data to disclose it in response to public records requests would risk facilitating criminal activity and exacerbating the opioid crisis.

#### **IV. CONCLUSION**

Accordingly, the United States respectfully urges this Court to find that the ARCOS data produced in this litigation is law enforcement sensitive and confidential, and asks the Court to order that the data not be disclosed in response to any state or local public records request.



Respectfully submitted,

DAVID A. SIERLEJA  
First Assistant United States Attorney  
Northern District of Ohio

/s/ James R. Bennett II  
JAMES R. BENNETT II (OH #0071663)  
KAREN E. SWANSON HAAN (OH #0082518)  
Assistant U.S. Attorneys  
Carl B. Stokes United States Courthouse  
801 West Superior Avenue, Suite 400  
Cleveland, Ohio 44113-1852  
(216) 622-3988 (Bennett)  
(216) 622-3851 (Swanson Haan)  
E-mail: James.Bennett4@usdoj.gov  
E-mail: Karen.Swanson.Haan@usdoj.gov

ALEXANDER K. HAAS  
Special Counsel to the Assistant AG, Civil Division  
ALICE SHIH LACOUR  
ERIC J. SOSKIN  
Counsel to the Assistant AG, Civil Division  
United States Department of Justice  
950 Pennsylvania Ave., NW  
Washington, DC 20530  
(202) 353-8679 (Haas)  
(202) 514-3180 (LaCour)  
(202) 514-1500 (Soskin)  
E-mail: alex.haas@usdoj.gov  
E-mail: alice.s.lacour@usdoj.gov  
E-mail: eric.soskin@usdoj.gov

**CERTIFICATE OF COMPLIANCE**

Pursuant to Loc. R. 7.1(f), I certify that the foregoing brief is fifteen (15) pages in length and within the length set by order of the Court.

/s/ James R. Bennett II

JAMES R. BENNETT II

Assistant U.S. Attorney

*Attorney for the United States of America*

**CERTIFICATE OF SERVICE**

I certify that, on June 25, 2018, I filed a copy of the foregoing Brief in Support of Objections electronically. The Court's electronic filing system will send notice of this filing to all parties. Parties may access this filing through the Court's system.

/s/ James R. Bennett II

JAMES R. BENNETT II

Assistant U.S. Attorney

*Attorney for the United States of America*