Bloomberg BNA

Pharmaceutical Law & Industry Report®

Limitations on Brand Protection Intelligence Sharing With Law Enforcement



BY RYAN GUILDS, ALEX BEROUKHIM, AND JAMES CONOLLY

Many pharmaceutical companies have developed strategic relationships with law enforcement in an effort to combat the illicit trade in pharmaceutical products. Proactive pharmaceutical companies understand that their assistance can enhance law enforcement's efforts through cross-sharing of investigative intelligence and information. Indeed, pharmaceutical companies are uniquely situated to identify counterfeit or illicitly trafficked pharmaceutical products. This makes cooperation with law enforcement not only logical but critical. Information sharing is not, however, without obstacles and risks.

Federal law, largely rooted in privacy, limits a pharmaceutical company's ability to gather or access certain criminal information. Significantly, however, this same information, if sought through state or alternative public channels may well be available legitimately. An informed brand protection department can ensure that it obtains helpful intelligence regarding its brands without running afoul of laws limiting law enforcement's disclosure of certain data or from certain databases. This article provides a basic overview of the laws relevant to this inquiry and provides practical suggestions on how to avoid risk while maximizing the effectiveness of a brand intelligence programs that seeks to benefit from law enforcement cooperation.

Ryan D. Guilds, E. Alex Beroukhim and James R. Conolly are with Arnold & Porter LLP. Guilds is counsel in the firm's white collar litigation practice group in Washington. Beroukhim is a partner in the firm's business litigation group in the Los Angeles office. Conolly is an associate in the firm's white collar defense and business litigation groups in Washington.

Gathering Intelligence In Support of Brand Protection Efforts

Actionable and timely intelligence is critical to the success of any successful brand protection program. Pharmaceutical companies have a variety of options for obtaining information about the illegal activity involving its brands. For example, companies can review online pharmacy sites, and purchase their own purported product for examination. Using private human intelligence, companies can learn of brick-and-mortar locations where contraband product is sold, and can then conduct undercover purchases to gather information on what is being sold and by whom. Companies can also contract with data vendors that aggregate and compile data to run queries that may help to identify illegal activity.

In addition, companies can communicate directly with law enforcement personnel to exchange information. This form of intelligence gathering is not only useful but appropriate. Law enforcement and the public benefit from the subject matter expertise the brand owner provides, while the brand owner in turn benefits from ensuring that law enforcement is focused on investigating and prosecuting illegal activity associated with their products.

Laws Preventing Access to Law Enforcement Information

Public-private information sharing has limits that law enforcement must observe. Some of the criminal information federal agencies maintain, for example, is aggregated within federal criminal information repositories and is, as a general rule, prohibited from disclosure

 ISSN 1542-9547

to private third parties except under narrow circumstances.[1]

NCIC

Chapter 28, section 534 of the United States Code authorizes the Department of Justice (''DOJ'') to ''acquire, collect, classify, and preserve identification, criminal identification, crime and other records.'' 28 U.S.C. § 534(a)(1). This authority led to the creation of the National Crime Information Center (''NCIC'') within the Federal Bureau of Investigation (''FBI''), a computerized index of criminal justice information which is available to virtually every law enforcement agency nationwide, 24 hours a day, 365 days a year. The FBI's Criminal Justice Information Systems Division (''CJIS'') is the NCIC's primary document custodian. [2]

Information is fed into the NCIC as it is gathered by federal, state, local, and tribal law enforcement agencies all over the country. Each of these agencies is responsible for gathering, compiling, and maintaining its own information. Only the individual agencies can enter, modify, and remove their own records. Through a telecommunications network, the FBI provides the infrastructure for these agencies to feed into NCIC information gathered during investigations, arrests, seizures, and operations in their own jurisdictions. Through this network, participating agencies can then access information contributed by other agencies from around the country to assist with their own investigations and operation.

According to DOJ rules, however, once information has entered the NCIC, disclosure from the NCIC is limited and generally excludes disclosure to private parties (absent a specific confidentiality agreement, described below). 28 C.F.R. § 20.33(a). Specifically, parties authorized to access the NCIC may only disclose NCIC information:

- to ''criminal justice agencies for criminal justice purposes,''
- to ''federal agencies authorized to receive it pursuant to federal statute or Executive order,''
- for ''licensing or employment'' purposes pursuant to federal legislation,
- ''[f]or issuance of press releases and publicity designed to effect the apprehension of wanted persons,''
- ''[t]o criminal justice agencies for the conduct of background checks,''
- ''[t]o noncriminal justice government agencies performing criminal justice dispatching functions,'' and
- to private parties engaged with the federal government through specific confidentiality agreements for the purpose of assisting law enforcement.

Id. The authority to disclose ''is subject to cancellation if dissemination is made outside of the receiving departments, regulated agencies, or service providers.'' *Id.* § 20.33(b).[3]

The exception that allows for disclosure of the NCIC information to private parties is exceedingly narrow. It is limited to parties that have entered into a specific type of confidentiality agreement, described in the regulations, ''for the purpose of providing services for the administration of criminal justice pursuant to that agreement.'' *Id.* § 20.33(a)(7). The Attorney General must approve an agreement's addendum to ''limit the use of the information to the purpose for which it is provided, ensure the security of and confidentiality of the information consistent with [the NCIC regulations], provide for sanctions, and contain other such provisions as the Attorney General may require.'' *Id.* Private access is carefully circumscribed and subject to numerous checks.

DOJ regulations authorize individual states, when exchanging information, to issue their own operational procedures policies on use and dissemination of criminal information. *See* 28 C.F.R. § 20.21 (''States and local government will determine the purposes for which dissemination of criminal history record information is authorized by State law . . . .''). In practice, however, states have chosen to adopt statutes or regulations that prevent disclosure of criminal history information — as compiled by the Attorney General (which is to say, by federal law enforcement authorities) — to private parties.[4] In short, neither applicable federal or state law allows law enforcement to release criminal history information to a private third-party that was obtained directly from the NCIC database.

Even requests for NCIC information through the federal Freedom of Information Act (FOIA), a traditional means of acquiring government information, have been blocked. Indeed, while FOIA broadly allows public access to information in the hands of government agen-

[1] The Food and Drug Administration takes a leading role in working to remove counterfeit or illicitly trafficked drugs from the system, but it partners routinely with the Drug Enforcement Administration, FBI, National Intellectual Property Rights Coordination Center, and the White House's Intellectual Property Enforcement Coordinator. Internationally, the FDA works with the State Department and U.S. Agency for International Development (USAID) to carry through domestic enforcement efforts to diplomatic and development programs. ''Counterfeit Drugs: Fighting Illegal Supply Chains,'' Howard Sklamberg, Deputy Commissioner for Global Regulatory Operations and Policy, Food & Drug Administration, remarks before the Committee on Energy and Commerce, U.S. House of Representatives, February 27, 2014.

[2] NCIC houses information in 21 distinct files: 7 property files—containing records for articles, boats, guns, license plates, securities, vehicles, and vehicle and boat parts—and 14 person files. These person files include the Convicted Sexual Offender Registry, Foreign Fugitive, Identity Theft, Immigration Violator, Missing Person, Protection Order, Supervised Release, Unidentified Person, U.S. Secret Service Protective, Violent Gang and Terrorist Organization, and Wanted Person Files.

[3] The rules do, however, allow for individual criminal justice agencies to disclose to the public ''factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.'' *Id.*§ 20.33(c). As read, however, this regulation appears to refer to information a particular criminal justice agency has either gathered or generated itself, rather than taken from the NCIC. Even so, if private companies are permitted to seek information that may fall within this exception the ''reasonably contemporaneous'' language provides a limited window of time in which to do so.

[4] *See, e.g.*, Cal. Penal Code § 11105; Fl. St. Ann. § 943.0542; and N.Y. Comp. Codes R. & Regs. Tit. 9, § 6051.1.

  PLIR ISSN 1542-9547

cies, the Act built in exceptions to prevent disclosure of information that may invade privacy (5 U.S.C. § 552(b)(7)(C)) or compromise law enforcement investigations, including the disclosure of confidential sources (5 U.S.C. § 552(b)(7)(D)). These two broad exceptions allow the federal government to refuse requests for disclosure of information housed in the NCIC and related federal databases.

Significantly, the law prevents disclosure from the NCIC database. But it does not prevent that same information from being shared if it is not obtained from the NCIC database. The law speaks to the source and not the substance of the information. For example, law enforcement may debrief an individual who has actionable intelligence regarding an illegal counterfeit pharmaceutical syndicate. Information obtained in that debrief could be shared with private industry because it was not obtained from the NCIC database. This is true even if the information is also housed in the NCIC database.

In their interactions with law enforcement, private parties should be careful to avoid receiving information that has come from the NCIC database. Notably, most criminal and civil penalty statutes for disclosing criminal history information are aimed at the government party responsible for the disclosure.[5] Even so, a private party receiving such information could face direct liability in some jurisdictions, such as California[6], or potentially accomplice or conspiracy-based charges for being party to the disclosure.[7] This is, of course, to say nothing of the reputational harm a company could suffer if it was seen as complicit in receiving improperly disclosed information. Companies should therefore make clear, in their interactions with agencies having access to NCIC information, that they do not seek, or do they want to receive, such information when it comes directly from the NCIC database.

The difference between being able to obtain investigative information and being prevented from doing so, is a matter of where that information is held. Criminal information gathered at the state level may be passed to federal law enforcement agencies, where it becomes part of the NCIC and other federal databases, and is beyond private reach when obtained directly from the database. The information itself, however, may still be available directly through the state law enforcement agency that gathered it — it just cannot be retrieved from the NCIC. Therefore, if a company became aware that it needed information generated in a particular jurisdiction, the company should consider obtaining the information through state-level contacts where permissible.

Tax Return Information

Tax returns, and the information contained therein, are generally prohibited from disclosure to private parties. The tax statutes prohibiting disclosure specifically are aimed narrowly at officers and former officers who would encounter such information in the course of their duties. In addition, however, the tax statutes contain provisions creating liability for private parties who willingly receive or publish tax information they are not authorized to have. *See* 26 U.S.C. § 7213(a)

The central tax statute, 26 U.S.C. § 6103, prohibits disclosure of tax returns, as well as related information and documentation, by any (current or former) officer or employee of the United States, any State, law enforcement agency, child support agency, local agencies described in the statute, or any other person who has had access to returns or return information. Section 6103's disclosure prohibitions extend far beyond individual tax returns. ''Return'' and ''return information'' include potentially any piece of information that could go into calculating, explaining, or excusing an individual's tax liability or that might be submitted to the Internal Revenue Service for any tax-related purpose.[8] Moreover, Congress defined ''disclosure'' under this Section broadly as ''the making known to *any* person in *any* manner whatever a return or return information.'' 26 U.S.C. § 6103(b)(8) (emphasis added).[9]

---

[5] *See e.g.* 18 U.S.C. § 1905 (providing that it is a misdemeanor offense for an ''officer or employee of the United States'' to disclose confidential information concerning the identity of an individual); 28 C.F.R. § 20.25 (providing for fines on an agency or individual improperly disclosing criminal history information); Cal. Penal Code §§ 11141-42; Va. Code Ann. § 9.1-136 (providing a misdemeanor offense for obtaining criminal history record information under false pretenses or unlawful dissemination of such information).

[6] *See* Cal. Penal Code § 11143 (providing criminal liability for individuals who receive or possess criminal history information knowing they are not authorized by law to receive such a record).

[7] *See, e.g. United States v. Jordan*, 582 F.3d 1239, 1244-45 (11th Cir. 2009) in which the government charged defendant Albert Jordan, a private practice attorney, with conspiracy to convert public property by receiving information from the NCIC, in violation of 18 U.S.C. § 641 (conversion of public money, property, or records). The government additionally charged Jordan directly for violating Section 641, by receiving a ''thing of value of the United States, that is, information contained in the NCIC records,'' which he was not authorized to possess. *Id.* at 1246. While the government did not charge Jordan with conspiracy to violate the disclosure provisions related to the NCIC, this case did establish at least one basis on which the government can take action against receipt of NCIC information.

[8] Section 6103(b)(2) defines ''return information'' as ''a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,'' and also includes specific agreements and documentation between the taxpayer and the Secretary of the Treasury.

[9] In *Mallas v. U.S.* 993 F.2d 1111, 1121 (4th Cir. 1993), the Fourth Circuit determined that the same bar to disclosure extended to information otherwise available to the public. At present, there is a split among the Federal Circuits as to whether publicly disclosed tax return information loses its protection under 26 U.S.C. § 6103. *See, e.g., El-Fadly v. I.R.S.*, 1999 U.S.App. Lexis 24820, at *3-4 (9th Cir.1999) (''[O]nce tax return information enters the public domain, the taxpayer may no longer claim a right of privacy in the information.''); *Payne v. Levy*, 35 F. Supp.2d 951, 952 (S.D. Texas 1998) (holding that plaintiff's disclosure of his own tax return information in public filings put that information into the public domain and dissolved its confidentiality protections under 26 U.S.C. § 6103.)

Given the broad definition of ''tax return'' information, pharmaceutical brand protection departments may well come in possession of information that potentially falls within the definition of ''tax return information.'' Law enforcement or brand integrity investigations may capture sales records of a suspected entity, for example. While possibly containing information that could be used for anti-counterfeiting purposes, such records may also include information used to prepare that entity's tax returns.

Criminal liability may attach directly in the event that a private party receives confidential tax return information willingly by offering something of value to the disclosing party. *See* 26 U.S.C. § 7213(a). Section 7213(a)(3) provides criminal liability for any person who receives confidential tax return information without being authorized to receive it, then prints or publishes it without authorization. Section 7213(a)(4) adds liability for persons soliciting tax return information in exchange for anything of value. Since both of these sections require a willful act with regard to tax return information protected by Section 6103, companies can avoid liability by preventing investigative personnel from approaching current or former government employees with access to this type of information in the first place. As an additional precautionary step, however, companies should avoid printing or publishing tax return information if they are uncertain of the information's origin.

Even where the law does not impose direct criminal liability on private actors, there remains the risk of accomplice or conspiracy liability, and reputational harm to the company.

Critical to a brand protection departments' efforts to address the risk of improperly possessing tax return information is knowing the source of the information. Information obtained through private efforts separate and apart from all government entities is on safer ground. If the tax return information has been routed through government tax bodies at any time, however, it is more likely that the Government will view that information as falling within Section 6103's disclosure prohibitions.

Grand Jury Information

Government entities with knowledge of federal grand jury proceedings may not disclose information that is presented to a grand jury to private parties, or to other unauthorized government entities. Federal Rule of Criminal Procedure 6(e) prohibits disclosure of ''matters occurring before the grand jury, except as otherwise provided [in the Federal Rules of Criminal Procedure].'' This includes information that would reveal the strategy of the investigation, the nature of the evidence, and potential theories of the investigation. Part of the reason for the restriction is to prevent unwarranted privacy violations, thereby avoiding reputational harm to those who may be the subject of a grand jury proceeding.[10] The more significant reason, however, is the need for criminal justice agencies to keep confidential their strategies for prosecution and to defend the integrity of ongoing investigations.[11] While this may be frustrating to companies who have provided information that sparked a government investigation in the first place, courts have not recognized any exception to this Rule.

Not all information presented to a grand jury is confidential, however. Independent facts do not become protected simply by virtue of a prosecutor's presenting them. If a prosecutor shows a grand jury evidence of counterfeit pharmaceutical sales, for example, the fact that the prosecutor presented the information is confidential, but the underlying fact is not. *See e.g. United States v. Stanford*, 589 F.2d 285, 291 (7th Cir. 1978), cert. denied, 440 U.S. (1979) (holding that information generated independently from the grand jury process, even if shown to a grand jury, is exempt from Rule 6(e)'s prohibitions. In addition, information that has become a matter of public record since being introduced to the grand jury is likewise exempt from the confidentiality provisions. Even so, companies should avoid seeking information regarding facts presented to a grand jury proceeding.

Department of Motor Vehicle Information

Companies should be likewise wary of receiving information they suspect to have come from Department of Motor Vehicle databases. While most Departments of Motor Vehicles are considered state agencies, it is a federal statute, 18 U.S.C. § 2721, that governs the release of information held by them. Under this statute, a state's DMV may release to law enforcement, or to private parties working on law enforcement's behalf, ''highly restricted personal information,'' for the purpose of carrying out law enforcement functions. As a general proposition, state DMVs are restricted from disclosing personal information to private parties not working in a law enforcement support role.

It is possible that this information can eventually be disclosed to private parties, however. Whether or not state law enforcement entities may disclose the restricted DMV information is determined by individual state laws. In New York, for example, law enforcement may not disclose DMV information that could, if released, result in harm to individuals. N.Y. Pub. Off. Law § 87. California's parallel statute indicates that DMV home address records are not subject to public disclosure under California's Public Records Act at all, regardless of whether or not they have been shared with law enforcement. Cal. Gov't. Code § 6254(f). In order to focus information gathering resources properly, private companies should seek legal counsel regarding individual state restrictions on DMV information disclosure.

Information Available from State Law Enforcement Entities

Pharmaceutical companies looking for information from law enforcement entities will likely be most successful at the state level where state laws either expressly permit or alternatively do not expressly prohibit sharing with the public. For example, in California, Florida, and New York, state law permits police to disclose blotter reports, 911 tape information, arrest information, complaints and requests for assistance, and victim information generally, unless doing so would en-

[10] *See Douglas Oil Co. of California v. Petrol Stops Northwest,* 441 U.S. 211, 219 (1979).

[11] *See, e.g., Inspection of Safeguarding Grand Jury Material at the United States Attorneys' Offices,* August 1996, Report Number I-96-11, Department of Justice, Office of the Inspector General, Inspections Division.

  PLIR ISSN 1542-9547

danger the victim or invade personal privacy.[12] Generally speaking, those same states sometimes exempt from disclosure rap sheets (again, for privacy reasons), security procedures, investigatory files, and information related to confidential informants.[13] Knowing these laws is critical to a successful and compliant brand protection program that seeks to leverage law enforcement knowledge.

Best Practices

While the bulk of confidentiality provisions discussed above apply to the government entities holding the information, companies supporting law enforcement efforts will not want to jeopardize those relationships by receiving confidential information through their government contacts. For greatest effectiveness, companies should have in place safeguards for making sure they give and receive assistance in a manner least likely to create legal impropriety.

Below is a list of some best practices companies should consider when executing brand enforcement programs:

- Establish communications protocols between the company and public law enforcement entities. These protocols should specify not only who should be responsible for communications with law enforcement, but also how and what types of information will be transmitted.
- When engaging data vendors who aggregate, or access, data from law enforcement entities, draft contractual provisions requiring the vendor to restrict access to information from federal criminal databases or confidential personal information.
- Develop clear directives that can be easily reproduced that highlight the company's commitment to complying with laws regulating the sharing of investigative intelligence with private parties.
- Draft provisions into contracts with third-party investigators indicating the company's expectation that the investigator will not access or convey to the company information which neither the investigator nor the company is authorized to have.
- Seek appropriate legal review before requesting information from law enforcement agencies in jurisdictions in which the company has not worked before.
- Develop training materials for brand protection employees, investigators and counsel describing what law enforcement information is available to the company and what is not. Focus on those jurisdictions where the company is most likely to interact with law enforcement.
- Be cognizant of the risks associated with obtaining tax return and grand jury secrecy information and administer training for brand protection personnel and vendors who may potentially interact with this type of information.
- Know the local laws in jurisdictions where you intend to informally receive information from law enforcement contacts.
- Create internal protocols for how to handle information received which the company does not believe it should have in its possession. This should include processes to divest the company of protected information it inadvertently received.

---

[12] *See* Cal. Gov't Code § 6254(f); N.Y. Pub. Off. Law § 87(2)(e)(i-iv); N.Y.C.R.R. 6150.4(b)(6); Fla. Stat. § 119.01 to 119.15; Fla. Stat. § 119.071(2)(c).

[13] Between states, there are some variations. In California, for example, the confidentiality of investigative files survives termination of the investigation itself. *Williams v. Superior Court*, 5 Cal. 4th 337, 362 (1993). In Florida, however, investigatory files may be disclosed once conviction and sentencing are final. Fla. Stat. § 119.071(2)(c); *see also State v. Kokal*, 562 So.2d 324 (Fla. 1990).