Bloomberg BNA

Pharmaceutical Law & Industry Report®

Privacy Considerations for Pharmaceutical Brand Protection Programs



By Ryan D. Guilds, E. Alex Beroukhim and Joseph G. Phillips

Privacy is big news these days, and it will only get bigger in the coming decade. In the United States, a few states recently passed laws restricting employer access to employees' Facebook and other social media accounts; California and Massachusetts continue to push the cutting edge of U.S. data privacy law; and some commentators mark 2014 as the year that Congress will pass national data breach notification standards, fueled by revelations of massive breaches of customer credit card data from Target. On the other side of the Atlantic, the European Union continues to mull proposed reforms to its already broad-ranging data privacy directive. China adopted new guidance on personal information protection last year, and new regulations pertaining to data privacy just took effect in March of this year. Elsewhere, countries from Mexico to the Philippines continue to implement national data privacy legislation.

Pharmaceutical companies need to be sensitive to this rapidly evolving legal landscape across all of their business functions and activities. Brand protection programs, however, present a unique set of privacy risks and issues, and companies would do well to be especially attuned to U.S. and foreign data privacy laws potentially affecting their brand protection initiatives. This article briefly surveys current data privacy laws in the United States and EU with emphasis on their application to the pharmaceutical brand protection space, notes some areas of potential growth in the law, and concludes with recommendations and best practices for compliance and risk mitigation.

Ryan D. Guilds, E. Alex Beroukhim and Joseph G. Phillips are attorneys 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. Phillips is an associate in the firm's business litigation group in Denver.

I. The Benefits of Corporate-Sponsored Brand Protection Programs

Counterfeiting of pharmaceutical products is a growing, global threat to public health, safety, and revenues. Counterfeit pharmaceuticals endanger patients when they contain too much, too little, or none of the active pharmaceutical ingredient ("API"), and when they contain toxic ingredients such as arsenic, leaded paint, and rat poison. Unintentionally low dosages of API risk creating drug-resistant strains of disease. Counterfeit drugs also fund criminal syndicates while simultaneously denying companies their deserved return on investment. Moreover, counterfeiting greatly undermines the reputations and profitability of entities in the legitimate supply chain, from manufacturers to pharmacies and doctors. Little wonder, then, that many pharmaceutical companies have robust programs designed to help combat this threat.

Brand owners' development of actionable intelligence concerning potential illegal activity in the supply chain is an important tool in the fight to protect a company's brand. Intelligence can be shared with the U.S. and international law enforcement community, which is generally very willing to receive such information, particularly if it is reliable and concerns high value targets. Gathered intelligence can also help to ensure that pharmaceutical companies have taken appropriate steps to protect their supply chains by incentivizing best practices and lawful activity with trade partners. Intelli-

 ISSN 1542-9547

gence can also support litigation, legislative reform, and track-and-trace initiatives as part of a comprehensive program designed to disrupt illegal activity and protect the legitimate supply chain.

Data Privacy Laws Relevant to Pharmaceutical Brand Protection Activities

Pharmaceutical brand integrity departments use a variety of investigative techniques—including surveillance, undercover operations, use of confidential informants, and internet takedown programs, among others—to gather information about traffickers. To be effective, these investigations must identify particular individuals involved with, and who can provide information about, illegal activity. The laws regarding the appropriate collection, retention, and use of personal data are therefore highly relevant. Knowing the risks and implementing controls to mitigate them is well worth the effort.

A. U.S. Federal Law

U.S. federal laws touching on data privacy[1] are perhaps most remarkable for what they do not do. Federal data privacy laws apply to government agencies, to certain types of information, and to certain industries or activities. For the most part, current federal data privacy law does not present major barriers to investigative brand protection operations.

1. Federal Laws Applicable to Government Agencies

Federal law restricts the government's maintenance and dissemination of personal information.[2] The Privacy Act of 1974 limits how, when, and about whom federal agencies can collect, store, share, and use personal information. The Driver's License Privacy Protection Act restricts state motor vehicle agency disclosures of motor vehicle records. While these laws may not apply directly to many brand owners, it is important that brand protection departments understand the limitations these laws impose upon law enforcement and other government entities with which they interact.[3]

a) Privacy Act of 1974

The Privacy Act of 1974 limits federal agency collection and disclosure of personal information and imposes storage and access requirements.[4] Agencies must limit the information they maintain to what is relevant and necessary to accomplish their purposes, must maintain their records accurately and completely, and must establish technical, procedural, and physical safeguards. To the greatest extent practicable, they must collect information directly from subjects and inform them of the agency's authority to collect the data, the intended purposes and routine uses, and the potential effects of not providing data. Agencies generally must limit their disclosures of personal information, and also must notify individuals of disclosures, permit individuals to inspect records pertaining to them, and allow individuals to request corrections or amendments to their records.

The Privacy Act likely does not prevent federal law enforcement agencies from sharing information with pharmaceutical brand protection departments in connection with legitimate law enforcement activities (including investigations of counterfeit pharmaceuticals). The Privacy Act allows agencies to disclose personal information for ''routine uses,''[5] provided that the routine use is published in the Federal Register.[6] ''Routine use'' means the ''use of [a] record for a purpose which is compatible with the purpose for which it was collected.''[7] When federal law enforcement agencies collect personal information about subjects of illegal pharmaceutical trade investigations and share it with pharmaceutical brand protection departments, this is almost certainly a ''routine use'' for which the information was collected.[8] Moreover, the Act specifically allows agencies to promulgate rules exempting materials compiled for law enforcement purposes from many of the requirements of the Act.[9] The provisions relating to legitimate investigative activities are generally so broadly drawn as to cover virtually any information likely to be shared with a brand protection department.

---

[1] Myriad federal and state laws govern the distribution of personal information by law enforcement agencies and personnel, including restrictions on who may access the National Crime Information Center (''NCIC'') database. These laws are outside the scope of this article.

[2] ''Personal information'' is a term of art that has different meanings in different contexts. Generally, personal information is information about an individual person such as a date of birth, ID number, or medical and financial information. The term ''personal information'' in U.S. law is not nearly so broad as it is in other countries, such as in the EU, where similar terms are meant to capture virtually any information that could be associated with a person.

[3] For example, the Social Security Number Protection Act of 2010 (''SSNPA'') restricts federal, state, and local agencies in two very specific ways. First, agencies may not display social security numbers, or derivatives thereof, on any check issued for payment by the agency. *See* Public Law 111-318 (amending 42 U.S.C. § 405(c)). Second, agencies may not employ, or contract to employ, prisoners in ''any capacity that would allow such prisoners access to the Social Security account numbers of other individuals.'' *Id.*

[4] 5 U.S.C. § 552a.

[5] 5 U.S.C. § 552a(b)(3).

[6] 5 U.S.C. § 552a(e)(4)(d).

[7] 5 U.S.C. § 552a(a)(7).

[8] The Federal Bureau of Investigation (''FBI''), for example, has published a notice in the Federal Register stating that information contained in its Criminal Case Files System—which includes a range of information on suspects, witnesses, etc.—may be ''disclosed as a routine use to an organization or individual in both the public or private sector if deemed necessary to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. An example would be where the activities of an individual are disclosed to a member of the public in order to elicit his/her assistance in our apprehension or detection efforts.'' *See* Office of the Federal Register, Privacy Act Issuances Compilation, available at http://tinyurl.com/mm58nzq; Federal Register, Vol. 63, No. 234, AAG/A Order No. 146-97.

[9] *See* 5 U.S.C. §§ 552a(j)(2) & (k)(2). As just one example, the Drug Enforcement Administration (''DEA'') has promulgated rules exempting its International Intelligence Data Base—which includes information on known and suspected drug traffickers—from various requirements of the Privacy Act. *See* Office of the Federal Register, Privacy Act Issuances Compilation, available at http://tinyurl.com/mm58nzq; Federal Register, Vol. 64, No. 219, AAG/A Order No. 179-99.

  PLIR ISSN 1542-9547

b) Driver's Privacy Protection Act

The Driver's Privacy Protection Act (''DPPA'') restricts state departments of motor vehicles (and their employees, officers, and contractors) from disclosing personal information connected to ''motor vehicle records.''[10] Significantly, the DPPA provides an exception to the limits on disclosure ''for use in connection with any civil, criminal, administrative, or arbitral proceeding . . . including the service of process [and] investigation in anticipation of litigation.''[11] To the extent that brand protection investigations legitimately can be characterized as conducted in anticipation of litigation or to further criminal proceedings, the DPPA likely does not prevent state DMVs from disclosing records to brand protection investigators.[12] Moreover, at least one federal court has held that database services like Westlaw® may collect information from DMVs and make the information available to third parties, including corporations, for those third parties' legitimate purposes.[13]

2. Federal Laws Protecting Financial Information

In addition to laws concerning certain kinds of actors (e.g. government agencies) and particular economic activities (e.g. web traffic of children)[14], federal law protects certain types of personal information. Federal laws touching on personal information privacy in the context of financial information may have unique application in the brand protection arena. The Fair Credit Reporting Act restricts disclosure of credit reports. The Gramm-Leach-Bliley Act imposes certain privacy requirements on financial institutions. And federal law limits access to tax information.

a) Fair Credit Reporting Act

The Fair Credit Reporting Act (''FCRA'')[15] restricts the disclosure of ''consumer reports,'' commonly called ''credit reports.'' ''Consumer reports'' include credit reports from major credit reporting agencies like Experian, but also include a broader range of information about a person when that information is meant to be used to determine a person's eligibility for employment or credit. The FCRA sets forth various circumstances in which obtaining and disclosing credit reports is permissible. Civil and criminal penalties apply to those who obtain and supply credit reports for purposes not allowed by the Act.

Brand protection departments must evaluate the types of information they receive to ensure compliance with the FCRA. Generally, investigators should avoid obtaining ''consumer reports'' as their receipt in the brand protection space likely does not satisfy any permissible purpose. At least one case has held that ''aiding in a private investigation of a suspected counterfeiter does not constitute a permissible purpose for acquiring a credit report of an individual.''[16]

b) Gramm-Leach Bliley Act

The Gramm-Leach-Bliley Act (''GLB''), also known as the Financial Services Modernization Act of 1999, is wide-ranging legislation concerning banks and other financial institutions.[17] GLB contains provisions concerning personal information privacy. Most notably, GLB requires financial institutions to provide consumers with privacy notices outlining the types of information they collect and disclose about those consumers, why and how information is collected and disclosed, and to whom it is disclosed. Consumers may opt out of certain disclosures, but not others.

Most relevant to pharmaceutical brand protection departments, consumers may not prevent financial institutions from disclosing information for purposes of combating fraud.[18] It is likely that financial disclosures covered by GLB and made as part of efforts to address counterfeiting and other relevant illicit activity fall within this exception. As a result, information database services such as Thomson Reuters' CLEAR® or Lexis Nexis' Accurint®—which in part collect consumer information from banks and other financial institutions—likely can re-disclose that information to corporate brand protection departments without risk of violating GLB. But risk remains. Notably, case law and agency guidance do not clarify what type of fraud the exception requires (i.e., bank fraud only, or broader efforts to combat fraudulent activity). Public policy favors disclosing such information to help combat the illicit pharmaceutical drug trade. Moreover, the risk that brand protection departments would use such information to perpetrate identity theft or other crimes—a major concern of the GLB privacy rules—is small. Still, brand protection managers and their law support should be aware that the issue remains an open one.

c) Receipt of Tax Information

Pharmaceutical brand protection departments should be cautious about receiving tax information. The Internal Revenue Code (''IRC'') prohibits federal employees from disclosing tax returns or tax return information.[19] Return information is ''a taxpayer's identity, the nature, source, or amount of his income . . . or any other data, received by, recorded by, prepared by, furnished to, or collected by the [Treasury] Secretary with respect to a return.''[20] Private entities and individuals can be liable

---

[10] 18 U.S.C. § 2721(a) & (b).

[11] 18 U.S.C. § 2721(b)(4).

[12] The DPPA allows disclosure ''For use by any licensed private investigative agency or licensed security service for any purpose permitted under'' the Act. 18 U.S.C. § 2721(b)(8).

[13] *See Young v. W. Pub. Corp.*, 724 F. Supp. 2d 1268, 1272 (S.D. Fla. 2010) (holding that it did not violate the DPPA for a state DMV to disclose motor vehicle record information to West Publishing Corporation, which in turn makes that information available for permissible purposes through online services).

[14] The Children's Online Privacy Protection Act (''COPPA'') imposes restrictions and obligations on operators of websites ''directed at children,'' and website operators who know they collect information from children. *See* 15 USC §§ 6501-6506. This article does not cover COPPA, as it has little relevance to most pharmaceutical brand protection operations.

[15] *See* 15 U.S.C. § 1681 et seq.

[16] *Boothe v. TRW Credit Data*, 557 F. Supp. 66, 70 (S.D.N.Y. 1982).

[17] *See* Public Law 106-102.

[18] *See*16 C.F.R. § 313.15(a)(2)(ii).

[19] *See, e.g.*, IRC §§ 6103, 7213A & 7431.

[20] IRC § 6103(b)(2).

for soliciting or publishing such information. At the margins, what counts as ''tax return information'' is a fact-specific analysis, and the law is not entirely clear. Some basic guidelines are that pharmaceutical brand protection departments should be wary of information relating to taxpayers—such as shippers, warehouses, chemicals manufacturers, or other entities of interest—in their capacities *as* taxpayers, especially when receiving information from an agency of the Treasury Department. Investigators should not solicit such information, and especially should not offer compensation in exchange for such information. Brand protection departments should not print or publish such information.

B. U.S. State Laws

Most states have similar, basic privacy laws concerning data breach and notification, data security, and social security number protection. Generally, these laws apply to entities which ''own or license'' personal information. Significantly, owning or licensing personal information is roughly equivalent to possessing that information.[21]

''Personal information'' is nearly universally defined in these laws as an individual's first name (or first initial) and last name combined with that person's social security number, driver's license or state identification number, or financial account or credit card numbers or passwords. Some states also include medical or health information, and California also recently added online login credentials to its list. In no state does ''personal information'' include public information lawfully made available through government records.

State laws impose duties on entities possessing personal information, which generally fall into three categories:

- **Duty to notify**. The duty to notify individuals and authorities of data breaches is a common state law requirement. Prototypical data breaches include situations in which information is stolen from an entity's computer system, is inadvertently left in a cab or other public place, or is used or disclosed for purposes unconnected to the entity's legitimate business. Routine discussion and use of personal information for everyday, legitimate purposes of pharmaceutical brand protection programs does not qualify as a ''data breach'' to ''unauthorized individuals,'' nor would disclosures to law enforcement or to private investigators.
- **Duty to destroy**. Some states have a duty to destroy, which requires complete and effective destruction of personal information when that information will be discarded. This requirement essentially means that entities must dispose of personal information in such a manner that it cannot be used by identity thieves.
- **Duty to protect**. Some states like California also have an affirmative duty to protect personal information, which means that entities must take reasonable precautions to protect personal data in their possession.

Many states also have laws restricting the disclosure or public display of social security numbers (''SSN''). Broadly, under these laws, no person, business, or other entity may intentionally make an individual's social security number available to the general public. While most brand protection activities involving SSNs likely do not qualify as making that information available to the general public, it is important that any brand protection program obtaining SSN information consider how this information is maintained and shared. And it is noteworthy that state law frequently places a higher degree of protection on SSN information.

C. European Union

The European Union data protection regime creates financial, criminal, and reputational risk for operations subject to its rules. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the ''Directive'') establishes the EU's overarching data privacy rules, which member states implement through (somewhat varying) national legislation and administration.[22] The rules are broad and complex; the Directive mandates protections for almost any kind of information about identifiable individuals in a wide range of contexts.

Very basically, the collection and transmission of personal data by companies ''established'' in the EU or using ''equipment'' in the EU is generally subject to strict limits on a company's ability to gather, use, store, and disclose a wide range of data. Special restrictions on processing certain types of data, such as criminal histories, are especially relevant to any pharmaceutical brand protection operations in Europe or involving European targets. A threshold question, then, is whether a given brand protection department has operations sufficiently ''established'' in the EU to fall under the rule.

In addition, the Directive restricts transfer of personal data to the United States because U.S. law does not provide an ''adequate level of protection'' for personal data. To help deal with the practical problems inherent in this restriction, shortly after the Directive became fully effective the United States and relevant EU authorities negotiated a ''safe harbor'' agreement by which participating U.S. companies would be deemed to comply with the Directive, therefore permitting transfer of data from EU countries to the U.S. companies.[23] A company's failure to comply with its safe harbor requirements is actionable by the US Federal Trade Commission as a ''deceptive trade practice.''

[21] Any business or department, including a pharmaceutical brand protection program, which operates in a given state and possesses information about state residents likely qualifies as an entity which ''owns or licenses'' personal information. Some states, including Illinois, do not limit the scope of these laws to entities which operate within the state. Instead, those states simply impose requirements on any entities which possess information concerning those states' residents.

[22] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at <http://tinyurl.com/6gpkrav>.

[23] Generally, companies that enlist in the safe harbor must (1) provide notice of their information practices; (2) afford data subjects some control over the use of their data; (3) limit further transfer of data only to entities which adhere to the safe harbor principles; (4) permit data subjects to access and amend their data; and (5) implement mechanisms to enforce compliance with the Directive's principles and to provide redress for injured data subjects.

  PLIR ISSN 1542-9547

Notably, the EU data protection regime is undergoing a comprehensive overhaul. New rules—predicted to take effect in 2016—are slated to update the current regime and impose regularity across the EU. Of special concern to brand protection operations are proposals to expand the jurisdictional scope of EU data protection law, including proposals to base jurisdiction upon the nationality of a data subject rather than the location of the data collector/controller. Because investigators may not know the nationalities of persons whom they are investigating, this type of rule could be especially vexing for brand protection operations outside Europe.

II. Recommendations and Data Privacy Best Practices

Several general practices and policies may help to ensure that pharmaceutical brand protection programs remain in compliance with privacy law.

As an initial matter, brand protection managers and company information officers would do well to recognize that brand protection activities likely trigger the application of myriad U.S. and foreign data privacy laws. Broader company-wide policies concerning data breach monitoring, protection, and response should incorporate brand protection personnel and activities. Brand protection personnel should be trained on the laws, and educated on steps necessary to protect personal information and to respond appropriately to any unauthorized disclosure.

Pharmaceutical companies should also recognize that brand protection departments receive personal information in unique ways distinct from other business units. Information exchange with law enforcement agencies is critical to the success of many brand protection programs. Yet while law enforcement may share personal information with private companies in support of efforts to combat illegal activity, the law in this area remains unsettled. There is also reputational risk in the receipt and use of personal information provided by law enforcement to a private company. Any personal information received from law enforcement should be treated as confidential, its receipt should be appropriately memorialized and explained, and its dissemination should be limited to personnel with a need to know.

Because certain information enjoys special protection, brand protection programs should consider ways to appropriately identify and mitigate the risks in these areas. For example, brand protection managers may want to conduct integrated and comprehensive legal reviews of their receipt of SSN and tax, drivers license, and consumer report information, and establish business rules for their acquisition (or avoidance thereof). To the extent that legal compliance hinges on the information's being received in support of the company's anticipated litigation, companies would benefit from adequately memorializing this purpose in investigative reports and summaries. Training brand protection personnel on what types of information they can and cannot obtain will help mitigate the legal and reputational risks associated with collecting and maintaining personal data.

Brand protection managers and law support should also take steps to reduce the risk of creating and duplicating personal information. Investigators should consider using code names for suspects and other individuals whenever full names are not necessary. Documents combining first and last names with other information can be especially sensitive under state law. Programs may retain and collect such information when necessary, but possession likely triggers certain obligations, such as the duty to notify affected individuals of unauthorized disclosure.

Data breach notification obligations, if triggered, can be especially awkward for brand protection programs because those programs most often do not want to alert the subjects of investigations to the fact that they are targets. Brand protection investigators should take steps to mitigate the risk of a breach. Avoiding the unnecessary transport of personal information is an important step. Brand protection personnel should also refrain from retaining sensitive information on personal computers, devices, and email accounts, and should transmit information in a secure manner and only to essential recipients. Third-party recipients should be informed of the need to protect personal information. And departments should also use secure disposal methods that completely destroy personal information.

Pharmaceutical companies should have data breach response plans in place before they ever experience a breach, including identification of the responsible internal team and potential third-party vendors such as forensic information technology specialists and credit monitoring services. Because of the unique issues raised in the brand protection context, companies should consider integrating the brand protection department into any broader data breach contingency plan, and that department may want to have its own specific plans and procedures as part of that structure.

Finally, brand protection departments must be cognizant of the relevant data privacy rules in foreign jurisdictions in which they operate. For example, the data privacy landscape in China—a major exporter of counterfeit pharmaceuticals—is shifting rapidly. China has recently implemented a variety of new rules pertaining to data privacy, and it remains to be seen how those rules will in fact play out in China's unique regulatory environment. As the laws in this area shift in many countries around the world, brand protection departments operating internationally should consider engaging local counsel to help account for the relevant rules in their overall data privacy compliance architecture.

III. Conclusion

Protecting pharmaceutical supply chains is important and necessary. Yet these activities implicate a variety of legal issues. Some laws in the brand protection space, such as those limiting pretexting and wiretapping, concern how investigators may obtain personal information. By contrast, laws touching on personal information privacy—the focus of this article—concern the type of information that can be received and what must be done with that information once it has been acquired. U.S. law is a patchwork of federal and state laws. States like California and Massachusetts continue to push for more data privacy protections, and for many purposes may therefore set the *de facto* compliance standards even as they pull farther away from the national norm. Brand protection operations will face an ever-multiplying host of data privacy rules in the coming years. And the United States is not alone in developing rules concerning the receipt and protection of personal information. The European Union and China are two important sources of law in this area, but they are not alone. Compliance will become increasingly complex,

and will depend on the development of comprehensive plans to identify and mitigate the risks in this area.

  PLIR ISSN 1542-9547