Discovering & Protecting Personally Identifying Information: The Basics

By Michael P. Lowry

With the increasing digitization of the world's information, it is becoming easier and easier for personally identifying information to be inadvertently disclosed. State courts are also implementing digitization programs, such as e-filing, to manage increasing caseloads and store documentation. Anyone with a Wiznet or PACER password can search these public documents for the information they contain, creating potential problems for counsel who file documentation containing personally identifying information. How may attorneys obtain the personally identifying information needed while protecting it, and themselves, from the risk of disclosure?

Nevada's definition of personally identifying information

NRS 239B.030(4) provides discretionary authority for governmental agencies, including courts, to require from a person who "records, files or otherwise submits any document to the governmental agency to provide an affirmation that the document does not contain personal information about any person or, if the document contains any such personal information, identification of the specific law, public program or grant that requires the inclusion of the personal information." Personal information covered by this affirmation includes:

> [A] natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
>
> 1. Social security number.
> 2. Driver's license number or identification card number.
> 3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.
>
> ~The term does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public.

NRS 603A.040.

It is unclear what the consequences of a breach of the above might be, but an example of the importance of protecting personally identifying information is the 2011 Nevada Legislature's enactment of SB 282. The bill appears primarily targeted at various forms of advertising. A violation is not only a misdemeanor offense, but also creates a private cause of action for the person whose social security number was "willfully and intentionally" disclosed. In pursuing a private cause of action, "[t]he court may award actual damages, reasonable attorney's fees and costs to the person whose social security number has been willfully and intentionally posted or displayed in violation of this section." Although not directly applicable to an attorney, it is not beyond imagination that inadvertently disclosing a social security number of an adverse party could complicate the litigation.

Federal courts have implemented a requirement similar to NRS 239B.030(4). FRCP 5.2(a) provides specific privacy protections for such information:

> Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:
>
> 1. the last four digits of the social-security number and taxpayer-identification number;
> 2. the year of the individual's birth;
> 3. the minor's initials; and
> 4. the last four digits of the financial-account number.

FRCP 5.2(b) provides certain exemptions and FRCP 5.2(h) provides a waiver for when the person seeking the protections of the rule has already filed such information without redaction. Again, however, the impact of a breach is not stated.

Producing and using documents containing personal information

Attorneys routinely handle personal information of

this nature and must utilize it as part of their practice. In civil practice this occurs most frequently in discovery and motion practice.

How do I obtain this information from an adverse party?

Personally identifying information is routinely important in many cases. Understandably, however, some parties and their counsel are reluctant to provide it. When can personally identifying information be obtained in litigation?

The test in discovery is whether the information is relevant. Federal courts confronted with discovery motions have refused to permit the discovery of social security numbers based upon the motion before them, but the courts have not categorically ruled out the possibility that the social security numbers could be discovered if the need can be justified and other avenues to obtain the information sought through the use of social security numbers have failed.

In *McDougal-Wilson v. Goodyear Tire & Rubber Co.,* the court determined that a request for social security numbers from potential witnesses was not a request for relevant information because the witnesses could be located through other means. 232 F.R.D. 246, 252 (E.D.N.C. 2005). The Court reasoned that "Goodyear legitimately redacted social security numbers from documents it produced out of concern for its employees' and former employees' privacy." Because plaintiff received last known contact information (e.g., last known address and phone number), the production of social security numbers was not compelled.

In another case, a court again concluded that a request for certain personally identifying information sought information not relevant to the case. *Scaife v. Boenne* arose from a section 1983 claim wherein the plaintiff sought the defendant officers' "social security numbers, their current home addresses, their residences for the past ten years, and information about any children the defendants may have." 191 F.R.D. 590, 592 (N.D. Ind. 2000). Examining the requests in the context of the complaint, the court concluded that "[t]here is no relevancy in the defendants' addresses, social security numbers, and facts about the defendants' children to the allegations raised in plaintiff's complaint. Nor is there any basis on which to conclude that the sought after information would lead to the discovery of admissible evidence." *Id.* at 592–93. A court in *Chavez v. DaimlerChrysler Corp.* reached a similar conclusion in the context of a disparate treatment employment claim. 206 F.R.D. 615, 622 (S.D. Ind. 2002).

Courts are also protective of employee personnel files that contain similar information. The subjects of such files are often non-parties to the litigation. Those files commonly contain addresses, phone numbers, income information, medical histories, employment discipline, criminal records, and other sensitive, personal information having little or no relevancy to the issues in litigation. To permit wide dissemination of personnel files would result in a clearly defined, serious, and unnecessary injury to the privacy of the employee who is not a party to the lawsuit. Revelation of such information could cause economic or emotional harm. The files could also contain embarrassing material and they commonly contain confidential material. *Raddatz v. Standard Register Co.*, 177 F.R.D. 446, 447 (D. Minn. 1997) (citing an unpublished decision); *see also, Whittingham v. Amherst College*, 164 F.R.D. 124, 127 (D. Mass. 1995) ("[P]ersonnel files contain perhaps the most private information about an employee within the possession of an employer."). The court in *Raddatz* even stated that unhindered production of these materials should not be permitted under a confidentiality order as "the very act of disclosing an employee's sensitive and personal data is a highly, and frequently, an unnecessarily intrusive act—whether or not that disclosure is governed by the terms of a Confidentiality Order." 177 F.R.D. at 447–48.

Federal courts appear hesitant to force the disclosure of "personal information," at least as defined in Nevada, absent relevancy or necessity. Even when relevant and necessary, production of this information may be highly restricted. If your client is producing documentation containing such information, redaction and privilege logs are likely necessary.

How do I use this information?

If relevant and obtained, how do you use this information? Carefully. As noted, it is unclear what the consequences of a breach of either NRS 239B.030(4) or FRCP 5.2(a) might be. The rules must factor, however, into both discovery responses and many routine deposition questions. They should also be taken into account in what might be considered innocuous tasks such as submitting medical records in support of a petition to compromise a minor's claim as required by NRS 41.200(3). Taking steps to protect identifying information as required by statute and rule is not only respectful of the nature of the information and the adverse party's privacy interests, but may also be a prudent step for the attorney to protect himself from the risks of disclosure.

Handling and protecting personally identifying information is an integral part of the work performed by many attorneys. It may be the make-or-break information for your client's litigation. As emphasized by the Nevada Legislature and federal court system, handling that information appropriately is becoming increasingly important.

Michael P. Lowry is a civil litigation associate at the Las Vegas office of Thorndal Armstrong Delk Balkenbush & Eisinger.