COMMENTARY

Public Access to Government Records and How Transparency Protects Privacy

by Grayson Barber and Frank L. Corrado

A significant trend in the area of information privacy is a growing recognition that personally identifiable information has commercial value, but also carries risks when it is disseminated. Government records that have been considered 'public' are harvested for personal information about citizens, but there is no guarantee that the information was ever intended for public consumption, or even accurate. As government regulators begin looking to generate revenue for states by prosecuting deceptive online practices, the state government itself may legally be considered a publisher of personally identifiable information.

The state of New Jersey has become an active publisher of large amounts of information about its citizens, collecting a great deal of data for many different purposes, from vital records (births, deaths, etc.) to licenses (professional licenses, hunting, fishing licenses, etc.) to titles (boat, aircraft, and other vehicles) to court records (convictions, civil actions, any document attached to a filing). Many of these documents contain sensitive, highly personal information, such as health records, government employee information, and qualifications for firearm permits.[1] But citizens have no choice about whether to provide this information to the state; it is compulsory. One must make disclosures to the government in order to function in society.

Most people do not realize that almost every time they interact with the state, they generate a record that can be sold for purposes totally unrelated to governmental activities.

Traditionally, records stored in government buildings—from land use documents to divorce decrees—have been available upon request. Data aggregators use the rhetoric of open government to purchase these 'public' records, and indeed, to the extent digital records shed light on government operations, online access to information does serve the cause of "government in sunshine." In the spirit of open government, a number of nonprofit groups have launched efforts to make the government's 'raw' data available to the public.[2] As applied to personal information in state government databases, this approach has the ironic effect of exposing information about individual citizens while revealing little or nothing about government operations.

The authors nevertheless believe that this approach (*i.e.,* making the raw data available to the public) can be an effective device for protecting privacy. Publishing the raw data introduces a measure of transparency into what is now essentially a "black box" system.[3]

For example, the *Asbury Park Press* has taken it upon itself to purchase government records in bulk and post them online in a database called Data Universe. The records include property records and taxes, government payrolls, school performance report cards, crime reports, conviction records, and more.

As soon as it was launched, people started visiting the website, found at www.app.com/apps/pbcs.dll/section?Category=DATA, to check on themselves and their neighbors. This was the first opportunity citizens had to see the records the government maintained, and disclosed, about them. They also started asking for corrections to errors. The errors were not the fault of the newspaper; they were encoded in the government databases.[4]

For in-house counsel, this issue is significant because regu-

lation is looming on the horizon, and many common assumptions about personally identifiable information are being jettisoned. In the last year, a number of bills have been introduced in Congress, and the Federal Trade Commission (FTC) has made it clear that it will invoke its consumer protection authority with respect to privacy concerns. Senator Patrick Leahy's proposed Data Privacy Bill of 2011, for example, establishes a national breach notification standard, and requires businesses to safeguard consumer data and allow consumers to correct inaccurate information.[5]

A number of common assumptions about government records should be reconsidered. The first assumption is that if the personal records were sensitive, the government would not make them public. But this isn't really so. In practice, the government records are repackaged for sale, and many are combined with other databases to create employee background checks, consumer profiles, and estimates of creditworthiness.

The second assumption about government records is that they are accurate. Data aggregation companies like LexisNexis, Acxiom, and ChoicePoint rely on this assumption when they extract information from government records for the products and services they sell. They provide assurances that these products and services are reliable, based on an assumption that the data gathered from 'public' records is accurate.[6]

A third widespread assumption is that all information in the public domain is benign, and can therefore be used for any purpose. It is a fact of the computer age that data must be converted into numerical codes. People and families are sorted into categories, and bureaucracies must treat them as groups rather than as individuals. To make use of personal information from government files, data aggregators must decipher and interpret the codes and categories they receive. Personal information that was collected for a particular reason, presumably by governmental mandate, is repackaged and used for entirely different reasons, at the discretion of the data aggregator. This introduces a possibility, and even a likelihood of misinterpretation and error.

These three widespread assumptions do not withstand close examination. Government records contain sensitive information, including Social Security numbers, medical data, and information about children. Problems with accuracy abound. Information may be coercively obtained, and not always easy to interpret, especially when numerical codes are assigned to categories of information; hence, the records are not necessarily benign and cannot reasonably be used for every purpose.

Harmful Consequences of Inappropriate Disclosure

The assumptions about open government records have had pernicious results, ranging from the comparatively benign, as when unlisted phone numbers can be obtained from government records,[8] to the plainly harmful, as when abusers locate domestic violence victims. These results have not always been obvious, since no one scrutinizes the sale of government records to commercial entities. These transactions may have negative effects on people's lives, affecting their employment, healthcare, and financial well-being. For people with negative records, it may become harder to get a job, rent an apartment, and obtain credit.[9] For example, it is entirely possible to be listed as a criminal because of a speeding ticket.[10]

The federal Privacy Act of 1974 embodies a set of principles that have been widely accepted in the United States and abroad.[11] Commonly known as the principles of fair information practices, they emphasize transparency and accountability:

- *Collection limitation:* There should be limits to the collection of personal data, and this data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the subject;
- *Purpose specification:* Personal data should be relevant to the purposes for which they are used and, to the extent necessary for those purposes should be accurate, complete, and kept up-to-date;
- *Use limitation:* Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the purpose-specification principle except: a) with the consent of the data subject; or b) by the authority of law;
- *Security safeguards*: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure;
- *Openness:* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller;
- *Individual participation:* An individual should have the right to:
  1) Obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;
  2) Have communicated to him or her data relating to the individual within a reasonable time, and in a form that is readily intelligible to the individual;
  3) Be given reasons if a request made under subparagraphs (a) and (b) is denied, and be able to challenge such denial; and
  4) Challenge data relating to him or

her and, if the challenge is successful, to have the data erased, rectified, completed or amended;

- *Accountability:* A data controller should be accountable for complying with measures that give effect to the principles stated above.

In contrast to the federal system, in which the Privacy Act accompanies and complements the Freedom of Information Act, New Jersey's Open Public Records Act[12] (OPRA) makes no distinction between government information and personal information. The result is that state offices can perpetuate government in secret, designating their work as "advisory, consultative, or deliberative," while exposing personal information about individuals.

In 2009, the new Rule of Court 1:38 altered the *status quo*. With respect to its treatment of Social Security numbers (SSNs) and other personal identifiers, the rule acknowledged that court records are sold with personally identifiable information, and placed limits, for the first time, on the personal data that can be sold. Apparently, though the records had been sold in bulk for a long time, no measures had been taken to redact SSNs, until the *Asbury Park Press* forced the issue.

The Judiciary now issues a disclaimer, noting that it cannot guarantee the accuracy of the records it sells in bulk. An administrative determination by the Supreme Court, dated Sept. 1, 2009, states "case docket information released in bulk should include a general disclaimer stating that the Judiciary cannot guarantee the accuracy of all records and set those records may be subject to misinterpretation. Entities that obtain information in bulk from the Judiciary should be required to provide the same disclaimer when the information is further disseminated."

A major influence in the development of the new Rule 1:38 appears to have been the Supreme Court's decision in *Burnett v. County of Bergen*,[13] which dealt with the presence of SSNs in land title records. In *Burnett*, the Court ruled that SSNs must be redacted from land title records, at the purchaser's expense, before the records could be disclosed in electronic form.[14]

There is no incentive to update or maintain records that have been purchased from the courts. Once the government has published information about an individual, it cannot punish others who publish the same information when it is obtained by lawful means.[15]

Transparency for Privacy

The authors believe the solution to the problem of privacy invasion is increased transparency with respect to government records. Government transparency serves individual privacy because it gives individuals an opportunity to find out how the state is treating their personal information.

The right to privacy confers, "as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[16] It encompasses an "individual interest in avoiding disclosure of personal matters,"[17] and a measure of control over "knowledge about oneself."[18]

This means that the government should refrain from disclosing sensitive personal information about its citizens, unless it has good reasons to do so.[19] Where there is a reasonable expectation of privacy in the information being disclosed, state agencies and courts should "decide whether the intrusion on the right of privacy is justified, balancing the governmental interest in disclosure against the private interest in confidentiality."[20]

As government agencies move from passively warehousing information to selling bulk records about individuals, fundamental questions arise about the government's relationship to its constituents.

It is important that the government recognize and accept its new role as a publisher, treating personal information in a manner that is fair to the individuals affected by its disclosure. This can be done using legal principles that are already codified in law—the fair information practices, discussed above.[21] These optimal data-handling practices do not pertain only to privacy, but to disclosure as well.

Conclusion

State governments have an obligation to do their utmost to ensure they collect limited information about their citizens, and that this information is accurate. As a necessary corollary, the public should have a right to: 1) know the government is collecting the information; 2) review the information; and 3) correct the information if it is inaccurate.

Transparency protects privacy when it gives individuals an opportunity to see information about themselves, a chance to correct errors, and a remedy when the information is misused. Transparency can be translated into public policy decisions that allow citizens, policymakers, and the media to assure themselves that a local, state or federal government agency is functioning as intended. ⚖

Endnotes

1. In Access and Aggregation: Public Records, Privacy and the Constitution, 86 *Minn. L. Rev.* 1137 (2002), Professor Daniel Solove observes:

> States maintain records spanning an individual's life from birth to death, including records of births, marriages, divorces, professional licenses, voting information, worker's compensation, personnel files (for public employees), property ownership, arrests, victims of crime, criminal and civil court proceedings, and scores of other [pieces of] informa-

tion...These records contain personal information including a person's physical description (age, photograph, height, weight, eye color); race, nationality, and gender; family life (children, marital history, divorces, and even intimate details about one's marital relationship); residence, location, and contact information (address, telephone number, value and type of property owned, description of one's home); political activity (political party affiliation, contributions to political groups, frequency of voting); financial condition (bankruptcies, financial information, salary, debts); employment (place of employment, job position, salary, sick leave); criminal history (arrests, convictions, traffic citations); health and medical condition (doctors' reports, psychiatrists' notes, drug prescriptions, diseases and other disorders); and identifying information (mother's maiden name, Social Security number). This list is far from complete.

2. In their paper Government Data and the Invisible Hand, 11 *Yale L.J.* 160 (2009), Professor Ed Felten, and his colleagues David Robinson, Harlan Yu, and William Zeller, argue the government should limit itself to creating a publicly available infrastructure for raw data, leaving it to commercial enterprise to develop the presentation software.
3. Frank Pasquale, Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing, in *The Offensive Internet*, edited by Saul Levmore and Martha C. Nussbaum (2010).
4. According to Paul D'Ambrosio, the *Asbury Park Press* will occasionally make corrections to the Data Universe database if it receives proof of errors in a record. Telephone conference, May 21, 2010.
5. Senators McCain and Kerry similarly introduced a proposed "Privacy Bill Of Rights."
6. The LexisNexis Consumer Access Program, for example, will supply an "Accurint Person Report" in response to a request for one's own file. *See* www.lexisnexis.com/terms/privacy/data/obtain.asp LexisNexis suggests that its records are the product of the latest technology and protected by law: "Please be reassured that both Accurint, and your personal information contained in Accurint databases, are regulated by the federal government and are subject to the Gramm-Leach-Bliley Act (15 U.S.C. §6801, *et seq*.) and the Federal Drivers Privacy Protection Act (18 U.S.C. §2721, *et seq*.)."
7. *See G.D. v. Kenny*, No. A-85-09, slip op. at 27 (N.J. Jan. 31, 2011) ("the practical obscurity of a file room now must coexist in a world where information is subject to rapid and mass dissemination").
8. *See* Special Report of the Privacy Study Commission on Home Addresses, www.nj.gov/privacy/special_directives_report_final.pdf.
9. *See, e.g.,* Evan Hendricks, *Credit Scores and Credit Reports: How the System Really Works, What You Can Do* (2004).
10. Brad Stone, If You Run a Red Light, Will Everyone Know?*, N.Y. Times*, Aug. 3, 2008, www.nytimes. com/2008/08/03/technology/03essay.html?_r=5&oref=slogin.
11. Privacy Act of 1974, 5 U.S.C. § 552a (1974) (fair information practices for personally identifiable information). *See also*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970) (permissible purposes of consumer reports); New Jersey Information Practices Act, N.J. Stat. Ann. § 17:23A-1 (1985) (governs HMOs and other insurance entities); Canada's Privacy Act of 1982, R.S.C. 1985, c. P-21. The Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection and Privacy of Transborder Flows of Personal Data are available on the OECD website at www.oecd.org/document/20/0,2340,en_2649_201185_15589524_1_1_1_1,00.html.
12. N.J. Stat. Ann. § 47:1A-1 *et seq*.
13. *Burnett v. County of Bergen*, 198 N.J. 408 (2009).
14. The expense of redacting SSNs is borne by the requestors, not the government. The cost to obtain public records is a significant obstacle to government in sunshine, but New Jersey's Open Public Records Act specifically provides that custodians may charge a fee for extraordinary expenses. N.J. Stat. Ann. § 47:1A-5(c).
15. *Cox Broad. Corp. v. Cohen*, 420 U.S. 469 (1974); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *G.D. v. Kenny*, No. A-85-09, slip op. at 44 (N.J. Jan. 31, 2011).
16. *State v. Hempele*, 120 N.J. 182, 225, 576 A.2d 793 (1990), *quoting Olmstead v. United States*, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting); *see also Doe v. Poritz,* 142 N.J. 1, 100 (2005); *Sterling v. Borough of Minersvill*e, 232 F.3d 190, (3rd Cir. 2000) (*quoting same*).
17. *Whalen v.* Roe, 429 U.S. at 599.
18. *U.S. v. Westinghouse*, 638 F.2d 570, 577, n.5 (1980).
19. An interesting description of the relationship of the government to its citizens is described in Neil M. Richards and Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 *Geo. L.J.* 123 (2007).
20. *Doe v. Poritz*, 142 N.J. 1, 78 (2005).
21. *See* U.S. Government Printing Office, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, July 1977. Europe and Canada treat freedom-of-information and privacy together. Every state in the European

Union has adopted the principles of fair information practices as law. *See* Council Directive 95/46/EC, 1995 O.J. (L 281), 31-51 (EC) (Directive of the European Parliament and the Council of Ministers of the European Commission on the protection of individuals with regard to the processing of personal data and on the free movement of such data); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2005), *available at* www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html. Canada's statute is called the Personal Information Protection and Electronic Documents Act, R.S.C., ch. P 21, §§ 10, 12 (1985).

Grayson Barber, *a privacy advocate, served on the New Jersey Supreme Court Special Committee on Public Access to Court Records.* ***Frank Corrado*** *is a partner at the law firm of Barry, Corrado, Grassi and Gibson, and president of the American Civil Liberties Union of New Jersey.* *The authors wish to thank Peter D. Meyers and Marc Rotenberg for their assistance in developing the arguments presented in this commentaryy. This article is based on "How Transparency Protects Privacy in Government Records," a longer web-published law review-style article.*