

## **Using Court Record Information for Marketing in the United States: It's Public Information, What's the Problem?**

**Karen Gottlieb, PhD, JD**

### Introduction

Your divorce was final last month and today you received a postcard from a local health club advertising a Ladies' Special membership. You have been thinking it is time for a "new you" and joining a health club would be a step in that direction. Is the postcard a coincidence, or good timing and smart marketing on the health club's part? It might not be a coincidence if you live in Ipswich, Massachusetts where the Probate and Family Court recently received a request from a local health club seeking the names and addresses of recently divorced women.

In most American jurisdictions, a court that gives away or sells personal information is not breaking any laws. Marketers can receive court record information directly from the court or buy the information from an information broker. Court record information is a veritable goldmine of marketing nuggets; divorced people need realtors to help them sell a house and maybe buy two new houses, drunken driving arrestees need defense attorneys, and bankruptcees need credit. Almost all information in court files is open to the public; exceptions usually are made only for juvenile court files and other information that is sealed, or specially closed to the public, by the court. But the sealing of personal information is a rare exception, not the rule.

For many decades, before there was an Internet or even high speed computers, there have been information brokers, like R.L. Polk & Company and Dun and Bradstreet, that collect court record information for resell.<sup>1</sup> Also, title companies, newspapers, credit bureaus, insurance agencies, and private investigators across the country have sent people to courthouses with paper and pencils, and more recently laptops, to collect information from court cases for their own use. This information includes civil judgments and money judgments on liens, divorce decrees, spousal and child support orders, bankruptcy creditors, and criminal convictions. Title companies need to know if there are liens against properties, newspaper reporters are hoping for interesting story leads, and credit bureaus are looking for just about any information to add to credit reports.

The legality and ethics of these secondary, or downstream, uses of court record information are rarely questioned, and if they are, the reply is sure to be, "it's public information, what's the problem?" The problem is your personal informational privacy is being invaded and you have no control over the dissemination and downstream use of

---

<sup>1</sup> R.L. Polk & Company sold their consumer marketing division to Equifax, one of the nation's three largest consumer credit bureaus, in 2000 for \$260 million. The division, Consumer Information Services, has self-reported demographic and lifestyle data on 180 million Americans and 105 million American households. Equifax has stated it will keep the consumer credit information separate from the consumer marketing information.

your own personal information. Most courts have not recognized that the underpinnings of the concept of public access to court records have changed due to technology, and that it is time to rethink the basic assumptions of public access. An electronic court record database is *more* than the sum of the individual court records. The personal information in these records can be compiled, aggregated, searched, and linked to other databases in a matter of seconds for a minimal cost and new information created. These databases require *more* privacy protection than individual records.<sup>2</sup>

This paper will address whether the use of personal information in court records for consumer marketing is a legitimate use of court record information and should be allowed to continue under the aegis of public access to court records.

### Why is this Personal Information Considered Public Information in the First Place?

Why is there no confidentiality in court records as there is for medical records? A cornerstone of American democracy is the administration of justice takes place in the open – a transparent government. Across the country, hearings and trials are open to the public with very few exceptions, and some are even televised. This common law right is rooted in medieval English law that was transported to the colonies and continues today. Somewhere between medieval England and now, this right for a person to have an open trial morphed into the public's right to inspect and examine (and copy for about twenty cents a page) the court records that document the open court proceedings. As court clerks began to have more and more of their records in electronic format, they realized personnel time spent at the counter providing files to information brokers, the media, and the general public would be decreased if the information was electronically transferred. The court could provide electronic downloads of these data in a high volume, or bulk, manner instead of pulling individual files one by one for a data collector or reporter to examine.

And many courts do exactly this. Title companies, credit bureaus, information brokers, and the media have contracts with courts to supply data downloads. The medium for transfer can be magnetic tape, CD, diskettes, or hard copy printouts. Even the companies that use the information internally will often resell, or trade, this information to other companies. With the advent of the Internet, a few courts have gone a step further and posted this information on the Internet for anyone to view and download.<sup>3</sup> The situation for personal informational privacy protection becomes even

---

<sup>2</sup> Latanya Sweeney Ph.D., a computer science and public policy professor at Carnegie Mellon University, has estimated 87% of Americans can be uniquely identified using only the information from the combination of birthdate, gender, and five digit zip code. By crosschecking data elements from an anonymized medical record database of Massachusetts state employees available to researchers and a public record voter registration list of Cambridge, Massachusetts, she was able to identify the medical record of William Weld, the then governor of Massachusetts. In effect, she re-identified anonymous (i.e., no name information) information. Earl Lane, A Question of Identity/Computer-Based Pinpointing of 'Anonymous' Health Records Prompts Calls for Tighter Security. In *Newsday*, November 21, 2000.

<sup>3</sup> In 2001, the Court Clerk of Manatee County, Florida uploaded all his scanned court documents to a court website accessible to the public for no charge. Searches on common names (e.g., John Williams) in the database turned up a great deal of personal information in the family court records. For example, a

more crucial as courts are moving toward either scanning or e-filing of documents. Now, the entire case file is electronic and can be uploaded to a court website in a matter of seconds with public access becoming public dissemination.

### What if the End Use is Marketing?

Much of the information from court records downloaded to third parties can be justified as legitimate end uses. The justice system is not served if civil judgments are never paid to the plaintiffs. And, fewer people would pay their civil judgments if there were no reporting to credit bureaus with the concomitant lowering of credit rating. An easily accessible database of divorce decrees keeps many men (and women) honest about their marital status. Also, the dissemination of criminal convictions can be seen as a public safety issue where the balance tips toward the public's right to know. But what of personal information in court files used for consumer marketing purposes?

The Acxiom Corporation<sup>4</sup> in Arkansas is an enigmatic company; most Americans have never heard of it, yet the Acxiom databases know a lot about most Americans. Acxiom collects personal data on 196 million Americans from public and private records and then "mines" the data to create consumer profiles to resell to marketers. They can link personal identifiers like name and zip code from varied sources: your subscription to Cat Fancy magazine, the purchases of gourmet cat food and an expensive brand of cat litter captured on your grocery store frequent shopper card, with the tax assessor's value of your house, to target you as a perfect candidate for a \$100 feline water fountain purchase. As an Acxiom executive stated, "The data has always been there. It's just that now, with the technology, you can access it."<sup>5</sup> He should have added, and sell it.

Consumers can control the dissemination of their personal information and prevent it from being swept into Acxiom's net (and the hundreds of other companies like Acxiom) by being prudent with their personal information. Put the Cat Fancy subscription in your cat's name, give incomplete (or incorrect) information on your frequent shopper's card, and use only your initials on the property assessor's records. These actions will make it difficult for data miners to link your personal information bits. And most importantly, read those privacy notices and opt out of the information sharing provisions. These are tactics very few people would have bothered with ten years ago, but now are becoming second nature to many.

---

paternity case was identified that stated the name of the mother, putative father, and child; dates of intercourse; and results of the paternity test. The Florida Supreme Court has since issued court rules that prohibit posting family law court file information on court websites and in November, 2003 called for a temporary moratorium to posting court documents online due to privacy concerns. Another website in Montgomery County, Pennsylvania posts its domestic abuse protection order database on the Internet and the database, which is searchable by abuser's name, contains names and addresses of the person petitioning for the protection order and any minor children.

<sup>4</sup> Acxiom is probably the largest consumer marketing information broker in the United States. It describes itself as "a company that blends data, technology and services to provide customer information infrastructure." In *Acxiom's Seven Privacy Principles for Business and Government*, Privacy and American Business Electronic Newsletter Vol. 10 (4), p. 9, April/May 2003.

<sup>5</sup> R. O'Harrow Jr, *Are Data Firms Getting Too Personal?* In the Washington Post, p. A1, March 8, 1998.

But personal information in court records is another story. There is no opting out of public access short of asking for records to be sealed. There are no privacy notices for divorce petitioners warning them the personal information in their petitions - the names and ages of their children, the abuse allegations, and financial information<sup>6</sup> - might wind up in a marketer's database. Personal injury plaintiffs are in a similar situation, a great deal of personal information must be disclosed for the court to resolve the dispute. Most people do not realize the information contained in the majority of court records is open to the public. They may suspect the grocery store is selling their buying information for marketing purposes, but they would never think their local court is giving away or selling their court information for a similar purpose. While the courts bemoan the lack of public trust and confidence in the justice system, most are not upfront with the public regarding the lack of privacy in their court records. It is a rare clerk's office that drives home the point that court records are public records and not only may be viewed by anyone, but are given or sold to third parties, and might wind up on the Internet.

There is evidence consumers would not be happy to learn their local courthouse records are available to marketers. A consumer privacy attitude survey conducted in 2003 by Privacy and American Business<sup>7</sup> shows the number of "Privacy Fundamentalists" has increased from 25% in 2000 to 36% in 2003. Privacy Fundamentalists are zealous about threats to their consumer privacy from business and favor active government regulation. Conversely, there has been a decrease in the percentage of "Privacy Pragmatists" from 63% to 53%. Privacy Pragmatists are consumers who balance the benefits against the risks of sharing their personal information. Privacy Fundamentalists are more likely to agree "Consumers have lost all control over how personal information is collected and used by companies" than are Privacy Pragmatists. Privacy and American Business, a business oriented think tank, interpreted this shift in privacy attitudes to another underlying factor, the increasing public concern about identity theft. This shift also can be interpreted as Americans becoming more cognizant of a "right to privacy in personal information", a right grounded in the ethical concept of autonomy that gives them the power to control the dissemination of information about themselves.

### State and Federal Policies and Rules

Is there a legal right in America to control the personal information in your court records and prevent the court from giving or selling your information to third parties for marketing purposes? It is important to note that the United States justice system is, at minimum, actually 51 separate, independent court systems – the federal courts and the state courts of the 50 states. The state courts themselves are all different in respect to court structure, organization, and amount of statewide centralization and

---

<sup>6</sup> Including how much you pay your psychiatrist every month, so much for medical information privacy in court records.

<sup>7</sup> Privacy and American Business, *Consumer Privacy Attitudes: A Major Shift Since 2000 and Why*. In Privacy and American Business Electronic Newsletter, Vol. 10(6), pp. 1, 3-5, September 2003.

standardization. By tradition, the clerks of the individual courts, not the judges, are the custodians of the court records,<sup>8</sup> and absent a court rule or state law, control the records. A state court clerk's control over the records greatly depends upon the degree of statewide centralization and whether court clerks are state appointed or elected. This situation leads to a great deal of variability both within and among states in regard to policies and rules on public access to court record information. The federal system is much more standardized, centralized, and tightly controlled by the federal judiciary. One commonality is all courts, state and federal, have records of interest to third parties for marketing purposes. The major distinction for our purposes is the federal courts have jurisdiction over bankruptcy cases and almost all family law and most personal injury cases are in state courts.

The federal courts do make all the documents in federal cases available for downloading by anyone for seven cents a page, 24 hours a day, 365 days a year on their PACER system. There are no restrictions except for registering with the system and the PACER group will help third parties write "scripts" that allow the downloading of data continuously. The PACER system went into effect before the federal judiciary created their policy on the downloading of personal information and each new wave of policy has been more protective of personal information. For example, minor children's names and birthdates are now redacted from bankruptcy filings.

Less than a third of the states have addressed bulk downloads of court databases and created written policies regarding end uses of court case information. This is due in large part to the fact bulk data electronic downloads historically have been limited to very basic information – parties' names, date of filing, nature of case – that would not raise privacy concern red flags. Downstream uses of bulk data downloads must be addressed now that more and more court documents (e.g., pleadings, discovery documents) might be in an electronic form and detailed personal information can be accessed easily.

Although some states (e.g., Arizona, California, Vermont, and Washington<sup>9</sup>) have thought long and hard about the privacy implications of posting court record information on the Internet and wrestled with balancing privacy and public access concerns, some decisions to post information on the Internet are made without weighing the pros and cons. This latter position is based on the rationale that public records, no matter what format they are in, are available for public inspection.

Many states were waiting for the *2002 Guidelines for Public Access to Court Records* developed by a joint committee of the Conference of Chief Justices and

---

<sup>8</sup> This situation dates to colonial times in America when judges were "circuit riders" and would travel from courthouse to courthouse in an area to hear cases. The stationary court clerk at the courthouse was the logical choice as keeper of the records. Judges still "ride the circuit" in rural counties in many states today.

<sup>9</sup> Washington has developed an expansive Access to Justice Technology Bill of Rights Initiative to create authoritative and enforceable standards of public access and privacy for the justice system. <[www.atjtechbillofrights.org](http://www.atjtechbillofrights.org)>

Conference of State Court Administrators to give them guidance.<sup>10</sup> The committee did address the issue of bulk downloads. The guidance is not protective of personal information in bulk downloads and states that all records that are publicly accessible are available for bulk distribution.<sup>11</sup> In commentary, the Guidelines make no distinction as to the end use of the data and give free rein to marketers to merge the court databases to their heart's content:

*Consistent with section 3.20, public access, including bulk access, is not dependent upon the reason the access is sought or the proposed use of the data. Court information provided through bulk distribution can be combined with information from other sources. Information from court records may be linked with other information and may be used for purposes that are unrelated to why the information was provided to the court in the first place.*<sup>12</sup>

California, which has a right to privacy in its state constitution,<sup>13</sup> has taken a more protective view of personal information in its court record public access policy. The court rules do not allow electronic remote access to records from family law, juvenile, guardianship, conservatorship, mental health, criminal, and protection order cases and limits bulk distribution to “electronic calendars, registers of actions, and indexes”.<sup>14</sup> Similarly, the state of Washington has taken a protective stance toward personal information in bulk data downloads and requires “data dissemination contracts” to control the use of downloaded court information by third parties:

*In order to effectuate the policies protecting individual privacy which are incorporated in statutes, case law, and policy guidelines, direct downloading of the database is prohibited except for the index items identified in Section III.B.6. Such downloads shall be subject to conditions contained in the electronic data dissemination contract.*<sup>15</sup>

A policy question that needs to be addressed is whether there are “legitimate” and “non-legitimate” uses of court record information. The traditional paradigm of *It’s public information* assumes there are no illegitimate uses of the information because it does not inquire into the end use of the information. But the traditional paradigm did not evolve in a world of Acxioms and 260 million dollar personal lifestyle and demographic databases. If the purpose of public access to court records is to ensure a justice system beyond reproach through public scrutiny of its’ activities, permitting court information to be used for marketing purposes tarnishes and cheapens the justice

---

<sup>10</sup> The Guidelines are available at <[www.courtaccess.org/modelpolicy](http://www.courtaccess.org/modelpolicy)>.

<sup>11</sup> § 4.30, CCJ/COSCA Guidelines for Public Access to Court Records.

<sup>12</sup> *Id.*, p. 30.

<sup>13</sup> There is no explicit “right to privacy” in the United States Constitution, rather the United States Supreme Court has construed a “right to privacy” that is akin to a “right to autonomy”.

<sup>14</sup> California Supreme Court, California Rules of Court, Rules 2070 to 2076.

<sup>15</sup> Washington Supreme Court, Data Dissemination Policy III(A)(2).

system. Court record information should be shared with third parties to ensure judgments are paid and sex offenders do not live across from elementary schools. Downstream marketing use is not a legitimate use because it does not promote justice and interferes with a person's right to control their personal information. Here the balance between public access and privacy tilts towards individual privacy.

Data dissemination contracts modeled on the compliance procedures of the Fair Credit Reporting Act<sup>16</sup> could be vehicles to ensure court record information is only used to promote and enhance the American justice system. A state could define permissible uses of court record information and these permissible uses would be stated in the data dissemination contract between the court and the original end user of the information. Also included in the contract would be compliance procedures requiring all prospective downstream users of the data certify the purposes for which they are seeking the information and certify the information will be used for no other purpose. The original end user would be responsible for ensuring that any downstream end user they shared or sold the information to would also be in compliance or the original end user suffers civil penalties.

Language from the Fair Credit Reporting Act fits the court information scenario very well and could be adapted by merely inserting court record information for consumer report and information broker for consumer report agency:

(e) Procurement of consumer report for resale.

(1) Disclosure. A person may not procure a consumer report for purposes of reselling the report (or any information in the report) unless the person discloses to the consumer reporting agency that originally furnishes the report

(A) The identity of the end-user of the report (or information); and

(B) each permissible purpose under section 604 [§ 1681b] for which the report is furnished to the end-user of the report (or information).

(2) Responsibilities of procurers for resale. A person who procures a consumer report for purposes of reselling the report (or any information in the report) shall

(A) establish and comply with reasonable procedures designed to ensure that the report (or information) is resold by the person only for a purpose for which the report may be furnished under section 604 [§ 1681b], including by requiring that each person to which the report (or information) is resold and that resells or provides the report (in information) to any other person

(i) identifies each end user of the resold report (or information);

---

<sup>16</sup> Fair Credit Reporting Act (FCRA) 15 U.S.C. § 1681e.

(ii) certifies each purpose for which the report (or information) will be used, and  
(iii) certifies that the report (or information) will be used for no other purpose, and  
(B) before reselling the report make reasonable efforts to verify the identifications and certifications made under subparagraph (A).<sup>17</sup>

## Conclusion

Privacy rights are at a turning point in the United States currently and developments in technology have brought these issues to the forefront. Although there are new federal restrictions on the use of credit reports (Fair Credit Reporting Act), driver license information (Driver's Privacy Protection Act), and medical information (The Privacy Rule of the Health Insurance Portability and Accountability Act), personal information in court records is still relatively accessible to anyone, including information brokers who mine the data for marketing purposes. The reason public access interests outweigh privacy interests is the paradigm – *It's public information* – is still firmly rooted in the court community. Cracks in the paradigm are appearing in the form of restrictions of downstream uses of the data, but they are only tiny cracks. Optimistically, these cracks will continue to grow and there will be a paradigm shift that protects personal information in court records and recognizes an individual's right to control the dissemination of his personal information.

---

<sup>17</sup> 15 U.S.C. § 1681e(e)(1) and (2).