

Public Records on the Internet: The Privacy Dilemma

Beth Givens, Director

Privacy Rights Clearinghouse
3100 5th Ave., Suite B
San Diego, CA 92103
Phone: 619) 298-3396
E-mail: bgivens@privacyrights.org
Web: www.privacyrights.org

INTRODUCTION

The Privacy Rights Clearinghouse is a nonprofit consumer information, research, and advocacy program based in San Diego, California. It was established in 1992 and is primarily grant-funded. The PRC operates a hotline, by telephone and electronic mail, and invites individuals to voice their complaints and obtain information about privacy matters. The PRC's many fact sheets offer practical tips on how to safeguard personal privacy. These are available on our web site, www.privacyrights.org.

One of the most challenging public policy issues of our time is the balancing act between access to public records and personal privacy. I will discuss the privacy implications of making public records available on the Internet, with emphasis on court records. I will conclude by offering some solutions for safeguarding personal privacy while upholding the public policy reason for providing access, that being to promote government accountability.

PUBLIC RECORDS ON THE INTERNET

Courts and government agencies at all levels of government – local, state, and federal – are increasingly making public records available on web sites. Some jurisdictions are just beginning, while others have done so since the mid-1990s.

There are two ways public records are accessible electronically. Some jurisdictions post them on their government web sites, thereby providing free or low-cost access to records. Government agencies

and courts also sell their public files to commercial data compilers and information brokers. They in turn make them available on a fee basis, either via web sites or by special network hookups. The following are examples of public records available remotely via electronic access.

- Property tax assessor files. Typical records contain name of owner, description of property, and the assessed value for taxation purposes. Some systems even provide blueprints of the property.
- Motor vehicle records – registration, licensing, and driver history information (varies by state).
- Registered voter files (restricted in some states).
- Professional and business licenses.
- Court files:
 - Case indexes
 - Tax liens and judgements
 - Bankruptcy files
 - Criminal arrest and conviction records, and warrants
 - Civil court recordings.

As I stated in the introduction, the reason that public records are public is unassailable — so we the people can monitor *our* government. Public records provide notice to all members of society of the official actions taken by government. They also provide notice of the “official” status of individuals and property. Making public records accessible to citizens via the Internet is a powerful way to arm people with the tools to keep government accountable.

But public records also contain a great deal of information about individuals, often very sensitive information. The following examples refer to court proceedings.

- Court records often contain Social Security numbers (SSNs) and financial account numbers. These are commonly available in divorce decrees, child custody cases, and bankruptcy filings. But when account numbers, personal identifiers, and dates of birth are accessible on the Internet, they could be used to commit financial fraud. The crime of identity theft is at epidemic proportions today, fueled in part by easy access to SSNs.
- Family law files typically contain information about children as well as allegations – whether accurate or not — of wrongdoing and negligence by warring spouses.
- When aggrieved insurance holders sue the insurance company over medical payment claims, the details of their medical conditions are likely to become part of the court record and thereby public. It is a common tactic of companies to threaten to bring highly sensitive medical information, as well as other personal matters, into the case in order to discourage the plaintiff from proceeding.

For example, in a prominent case of alleged identity theft negligence, the defendant, a credit bureau, obtained the plaintiff's gynecological records in order to attempt to show that she was mentally unbalanced and that her claims had no merit.

- In a dispute with a neighbor, or a business dispute, many allegations can be made that might not be true.
- In employment-related matters such as sexual harassment cases, it is common for the defendant to divulge extraordinarily damaging allegations about the plaintiff, such as lifestyle and sexual history.
- In criminal cases, the statements of victims and witnesses become part of the public file. These often contain highly sensitive personal information. Witnesses' personal safety can even be at risk in some cases if their identities are revealed.

It is important to note that in the majority of situations, providing personal information to government agencies and courts is *mandatory*. Individuals have little choice in the matter.

Providing access to public records on the Internet alters the balance between access and privacy that has existed in paper and microfiche records. Many commentators have used the term "practical obscurity" to describe the de facto privacy protection accorded court documents stored in back rooms and accessible only by visiting the court house and asking a clerk to retrieve them.

NEGATIVE CONSEQUENCES OF ELECTRONIC PUBLIC RECORDS

I predict that there will be significant negative consequences to individuals when public records are widely available on the Internet or via proprietary fee-based systems. I list eight such consequences here, and then conclude with suggested solutions.

1. Fewer individuals will choose to participate in government. There is the very real possibility that the continued growth of public records web sites and information services that compile government records from many sources will result in the chilling effect of people choosing not to take part in public life. If the result of participation in public life is to lengthen one's electronic dossier and make more personal information available to whoever wants to obtain it, then it is likely that people will avoid those situations where personal information is gathered.

A former California Secretary of State Tony Miller observed that many people do not vote because they do not want their name, address, party affiliation and other information publicly available. That is why his office promoted legislation – now law — to make the home address confidential. We have heard ample evidence from callers to our hotline to support his observation.

2. Justice will only be available to those with the resources and know-how to seek private judicial proceedings. Those who can afford to hire private judges will choose this option in order to keep their personal information out of the public records generated by the traditional court system. Only the rich will be able to safeguard their personal information in this manner. Many of those who do not have the means to hire private judges will choose not to file suit against their insurance company, for example, or their abusive employer. We may become a society in which only the rich get justice. Indeed, many say we already are.

3. As mentioned above, the crime of identity theft will be fueled by easy access to personal identifiers and other personal information via electronic public records.
4. Individuals will experience shame and embarrassment, even discrimination, when details of their personal lives are broadcast in court records available on the Internet.
5. Reputations will be destroyed because of errors. There is no such thing as a perfect data base. And there are no infallible users of data files. We are already seeing the growing problem of individuals who are wrongfully linked to crimes they did not commit. This occurs when an imposter uses an innocent person's identifying information when apprehended by law enforcement. Another scenario is when tax liens and judgements incurred by the identity thief are listed in the name of the innocent victim. In other situations, the investigator obtains information on the wrong John Doe, not taking adequate care to match the information with the correct individual. Another scenario is when the information broker's files are not up to date and the investigator, perhaps an employment background check company, is not informed of acquittals or dismissals.
6. Data from electronic public records files will be used for secondary purposes that stray far from the original public policy purposes for which they were first created, that being government accountability. Compiling public records information from several sources and merging them with commercial sector data files allows the data to be sifted and sorted in many different ways. Brand new records are created. The types of uses that can be made of these new records extend far beyond the original public policy reason for collecting them. A Utah court, for example, learned that a resort that catered to singles was accessing divorce files in order to obtain the names of individuals to receive its marketing solicitations.

But there are far more serious consequences to merging disparate electronic files of personal information into massive data bases. We are becoming a "dossier society." Extensive histories – whether accurate or not – are increasingly available at the click of the mouse to virtually anyone.

Law professor Jeffrey Rosen discusses the negative consequences of a dossier society in his 2000 book, *The Unwanted Gaze: The Destruction of Privacy in America*. His main concern is the compilation of bits and pieces of information about us from disparate sources, taken out of context, and then used to form conclusions and make decisions about us. He says:

...[W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences. (p.9)

He used the subpoenaing by prosecutor Kenneth Starr of Monica Lewinski's book purchases from a Washington, D.C., bookstore as an example of how such profiling can harm individuals. This occurred during the Clinton administration sex scandal. Rosen further states:

Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. (p.8)

7. A particularly troubling consequence of untrammelled access to electronic public records is the loss of "social forgiveness." In a dossier society, there is no social forgiveness. Your

conviction of graffiti vandalism at age 19 will still be there at age 29 when you're a solid citizen trying to get a job and raise a family.

There are precedents for restricting the amount of access to various informational histories. One is the rap sheet — or criminal history — which in California and many other states is confidential, not public. Juvenile court files are sealed, at least for those youth not tried as adults. On the private sector side is the credit report. Documentation of a bad payment history can only be kept on the books for seven years — a bankruptcy for 10 years. In these ways, society allows the possibility “starting over.”

8. As a consequence of all the factors I've raised here, I predict that our society will see a growing number of individuals who are disenfranchised for life. Large numbers will not be able to find employment because of negative information in court files — whether true or not — from years gone by. Or they will be relegated to lower-paying jobs in the service industries, unable to bring their true abilities into the employment marketplace. We have been contacted by many such individuals in our ten-year history. I believe, sadly, we will be contacted by many more.

SOLUTIONS

What can be done to mitigate the negative consequences of making public records available on the Internet and from other electronic services? Governments are not likely to make the decision to keep such records off the Internet. Indeed, they should not. The public policy reasons for making them available electronically are irrefutable — promoting easier access to government services as well as opening government practices to the public and fostering accountability.

But there are several approaches government agencies and court systems can take to minimize the harm to individuals when sensitive personal information is to be posted on the Internet.

First, court systems can start by posting only the court indexes, registers, and calendars on the web rather than the full texts of court proceedings.

Second, court systems can demand that the automation systems they procure are able to support flexible redaction features. Such systems should enable sensitive information to be tagged so that when the files are loaded onto the web site, it is blocked from view. If such systems are not yet available, court systems should wait until they are more widely accessible before posting the full-texts of court documents on the web.

Third, courts must adopt rules that prohibit the most sensitive of court files — including family law cases — from being posted in full on public web sites.

- The California Judicial Council has recently adopted rules of court (December 2001) that prescribe what types of records can and cannot be accessed electronically by the public. www.courtinfo.ca.gov/newsreleases/NR91-01.HTM

- The Justice Management Institute is currently in the process of drafting a model rule of court for remote electronic access to court files that can be adopted by state courts. www.jmijustice.org.

- The Judicial Management Council of Florida released a particularly thoughtful report in November 2001, “Privacy and Electronic Access to Court Records.” Its main recommendation

is that “[u]ntil policies are developed that appropriately balance privacy with access, and which support the core mission of the courts to do justice, unrestricted electronic access to court records should not be available.” (p.2) www.flcourts.org/pubinfo/documents/privacy.pdf.

Fourth, government agencies must ask themselves what public policy objectives they are accomplishing by making records available on the Internet. Would there be a way to limit the amount of information posted on the Net without undermining the public policy purpose of making public records accessible on the agency’s website? I suggested earlier, for example, that courts can choose to post only the case indexes on the Internet rather than the full-texts of files. Another example is already in practice. The San Diego County (California) Assessor decided to not post the *names* of property holders on its web site. Rather, users must seek property valuation data by searching under the *address* of the property. The primary use of this file, after all, is to determine the taxable value of property and to check that similar property is taxed at the same rate. Name searches are not possible via the web site, and indeed are not necessary.

The preceding recommendations pertain primarily to court and government agency records. We must also examine those professions that use public records information, namely information brokers and private investigators.

My **fifth** recommendation is to regulate the information broker industry. At present, information brokers purchase public records from local, state, and federal government agencies and repackage them for access by subscribers. They add data files from commercial data sources such as credit reports and consumer survey data. Virtually anyone can obtain access to these files, although many information brokers claim they limit access to professions such as private investigators, attorneys, law enforcement, media, debt collectors, landlords, and employment background checkers.

The information broker industry must be regulated much like the credit industry is regulated, under the Fair Credit Reporting Act (15 USC 1681). Individuals must be able to find out when information about them is accessed and for what purpose. They must be able to get access to those data compilations in order to determine if they are accurate. And they must be able to take legal action when personal data is obtained and disclosed for illegitimate purposes.

Sixth, the loopholes in the background check laws at the federal and state levels must be closed. The federal law is the investigative consumer reporting section of the Fair Credit Reporting Act (15 USC 1681d). This law requires employers to obtain consent from the subjects of background checks. If an adverse hiring decision is made, the individual must be given a copy of the report.

At present, the federal law only pertains to employers who hire third party investigators to conduct background checks. It does not apply if the employer conducts the background check itself. An increasing number of employers are doing their own investigations due to the availability of low-cost information broker data bases on the web. The law must be broadened to encompass employers who conduct their own searches. (The California Legislature amended its background check law, effective 2002, to require employers who conduct their own investigations to abide by the same disclosure requirements as third part investigators. California Civil Code 1786.53.)

The law must also close the “adverse decision” loophole. An employer might claim to have decided to not hire an individual because of a superior job pool, not because of negative information found in the background check. In such cases, the applicant does not need to be given a copy of the report and may never know that erroneous information, for example, may have been the real cause of

the rejection. Employees and job applicants must be given copies of their background checks in *all* instances, not just those where adverse decisions have been made. Of course, there must be an exception for investigations conducted when there is suspicion of criminal wrongdoing. To read more about the problem of background checks and wrongful criminal records, see a 2000 speech available on the PRC web site, www.privacyrights.org/ar/wcr.htm.

My **seventh** recommendation is to regulate the private investigator profession in those states where they are not now regulated. Further, the regulations must be tightened and made uniform nationwide, perhaps by federal law. Private investigators must be held to strong standards regarding their access to and use of sensitive personal information. They should be held accountable when they misuse personal information. It is the private investigative profession that is most often hired to conduct background checks.

My **eighth** and final recommendation is in the realm of the “impossible dream.” Even though it will be difficult if not impossible to achieve, it must be considered by all of us. We are going to have to transform how our society judges individuals – not an easy task. As I discussed earlier, we appear to be forgetting the older social value of “societal forgiveness.” If we are becoming a dossier society, and I don’t see signs suggesting otherwise, we must all strive for greater tolerance when “negative” information is found in personal data compilations. (One person’s “black mark” is another’s life lesson learned the hard way.)

How to accomplish such a societal transformation is hard to envision, especially at a time when we are increasingly a “get-even,” litigious society. For starters, schools and colleges must teach about tolerance and responsible information-handling practices in business and ethics classes. And employers must be willing to look beyond many of the so-called negative items found in background checks in their hiring decisions. I realize that the latter is especially difficult for companies to do given the likelihood of facing negligent hiring lawsuits if bad decisions are made.

CONCLUSIONS

As I said at the beginning, the balancing act between access to government records and personal privacy is one of the most challenging public policy debates of our time. We can mitigate many of the harmful consequences of making personal information available electronically if societal institutions are willing to take the steps I’ve suggested here.

A key recommendation is that government agencies take a “go slow” approach to posting public records on the Internet. The full texts of court records should not be posted until flexible and effective redaction technology is available, and until court systems have adopted rules that support sealing the most sensitive information.

Further, those professions that use public records must be more stringently regulated as a deterrent to using these data files negligently and abusively. Individuals who are harmed by negligent background checks or by illegitimate access to and dissemination of personal information must have meaningful legal recourse for their grievances.

Thank you for your thoughtful consideration of these matters.