



Balancing access and privacy

Free PACER

By Susan Lyons

In 2001, the Judicial Conference of the United States gingerly entered the Internet age with the release of a Web-based version of the Public Access to Court Electronic Records (PACER) database that allowed remote public access to most federal civil court documents over the Internet. It did so only after two years of studies, reports, and the solicitation of public comments. The 242 comments received by the conference reflected the tension between access and privacy. Journalists, private investigators, and data companies urged full and unfettered access, insisting that “public is public!” Other comments urged caution, citing privacy concerns and the potential for identity theft from the misuse of sensitive financial and personal information contained in many court filings.

The courts balanced these concerns by coming up with the system that remains largely in place today. Obtaining documents through PACER requires a password-protected account. Anyone can apply for an account but must surrender some personal information to do so: a physical address, an e-mail address, and credit card information. Account users pay a fee, now at \$.08 per page, to download documents. While charges only apply after the first \$10 of downloads and there is a cap of \$2.40 per document, the fees effectively discourage attempts to capture large sections of the database.

Social security cases, which typically contain private medical information, were excluded from the system, and court rules were changed to require some personal information, like Social Security numbers, to be redacted from court filings. Criminal cases were initially excluded, but after a pilot project that allowed access to criminal pleadings in 11 courts, access was expanded in 2003 to include widespread access to criminal filings.

PACER made its debut in the early 1990s as a dial-up service offering a limited selection of court documents over slow dial-up modems with charges of \$1 per minute. Its migration to a Web-based database in 2001 brought

court, have long been open to the public. Some authors argued that these paper records existed in a state of “practical obscurity” that served to minimize privacy concerns. Court records held in paper files are not easily browsed and potential identity thieves might feel some discomfort in lingering in the records room of a courthouse.

Judge J. Rich Leonard, a member of the Judicial Conference committee that formulated the policy on PACER, responded that the judiciary had weighed these concerns carefully in developing the program. Writing in the *American Bankruptcy Law Journal* in 2003, Judge Leonard notes that the account registration system provides some check on abusive use of court documents: “Remote access to federal court data is not anonymous. Instead, a proposed user must register with the PACER (Public Access to Court Electronic Records) Service Center and obtain a log-in and password and set up a billing account.... [A]n electronic footprint of each user who accesses any file is created. Although this may not prevent harm, there is some deterrent effect to misusing data from a federal court file when access can be traced to a particular password.”

The Free PACER Pilot Program

In November of 2007, the Administrative Office of the United States Courts (AOUSC) took another step toward full public access: in cooperation with the Government Printing Office, it began a two-year pilot program that offered free and unrestricted access to PACER at 17 libraries that were participants in the Federal Depository Library Program (FDLP). This article reflects on that brief pilot program, its abrupt suspension, and the continuing tension between privacy and access. It concludes with recommendations for how the courts can offer free access to PACER that is broadly accessible to the public while still protecting the legitimate privacy interests of litigants.

My library, an academic law library located in downtown Newark, New Jersey, volunteered for the two-year pilot program and was among the 17 libraries chosen to participate. Other participants included six other academic law libraries, state libraries, county and state court libraries, college libraries, a federal circuit court library, the Law Library of Congress, and a public library. Each library received a password for the free account. The terms of the pilot program dictated that we could only use the free PACER password on computers within the confines of the library. In my library, the government documents computer,

adjacent to our reference desk, was the main portal for PACER access. Only librarians and circulation staff had access to the password.

On the very day I received our password and while I was still working on a Web page that would promote the program and explain how to use PACER, the reference desk called to alert me that a patron had just come in asking to use our free PACER. My first customer told me he had just come from the federal courthouse, about a mile away from our library, where the clerks’ office had posted a copy of a press release from the U.S. Courts Web site about the free PACER program with the name of our library circled.

Over the next several months we received a steady stream of visitors who came to use the free PACER service. *Pro se* litigants were the largest group of users, many of whom were using PACER to keep track of what was happening in their own cases. Other users included attorneys, students, and an out-of-town journalist. Our busiest days brought three or four requests to use PACER. On other days there were no requests.

Overall usage averaged about 30 visitors per month, a level that was quite manageable for library staff. Each user had to be logged in by a library staff member, usually the librarian working at reference. Because PACER accounts have unwieldy user names and passwords with odd characters, this required taking out a piece of paper with the password and trying to type it in while concealing the password from the patron. A system that used IP authentication rather than passwords would have provided greater security and created less anxiety for the library staff members.

Our participation in the program continued unremarkably until late September of 2008 when all participating libraries received an urgent e-mail from the court administrator telling us to immediately change our passwords. After we all did so, we received another message stating that the pilot program had been suspended indefinitely. In a conference call, the court administrator informed participating libraries that there had been a security breach and that one or two of the pilot program passwords had been used to download a massive amount of documents.

In February of 2009, several newspaper accounts provided a fuller description of the incident that caused the AOUSC to abruptly suspend the free PACER program. Aaron Swartz, a 22-year-old computer whiz, managed to download nearly 20 million pages of PACER documents, or about 20 percent of the entire database, before the

improved access and also generated a flurry of articles in law reviews and bar journals on the merits and perils of the new system.

Some articles posed hypothetical situations wherein one’s identity could be stolen, or sensitive information could be used to blackmail individuals whose private information could now be accessed by anyone with a PACER account. Others warned attorneys that they might be liable for malpractice if they failed to carefully redact private information from court documents.

Of course, court records, with the rare exception of cases sealed by the

government shut down access to all free PACER pilot accounts. Swartz, who at the age of 14 was among the authors of the RSS 1.0 specification, was inspired by Carl Malamud's call for a "thumb-drive corps" to liberate PACER documents so they could be made freely available on the Web.

Malamud is the founder of Public.Resource.org, a nonprofit group working for open government. His earlier work helped to provide free public Internet access to Securities Exchange Commission (SEC) documents as well as patent and trademark databases. In an article in *Wired Magazine*, Malamud describes the PACER system as "the most broken part of our federal legal mechanism." *The New York Times*, in an article about the efforts of Swartz and Malamud to make court records more accessible, described PACER as a "system designed in the bygone days of screechy telephone modems. Cumbersome, arcane and not free, it is everything that Google is not."

Preserving Privacy

Clearly the greatest level of access the government could provide would be to make PACER freely available on the open Web, where search engines could index its 100 million pages, and researchers could apply Web 2.0 tools to analyze the data and develop custom applications. Congress is pressuring the courts to provide free access to PACER but also to ensure that private data is protected. Senator Joseph Lieberman, Chair of the Homeland Security and Governmental Affairs Committee, has asked the Judicial Conference why it continues to charge for PACER access and also demanded the courts do more to protect private data.

Congress' demand that PACER be free and accessible to all without compromising legitimate privacy interests or, in the case of criminal filings, anyone's security, puts the courts in a "Catch 22" dilemma. Before exploring whether there is a way out of the dilemma, it is useful to consider if there is something about PACER documents that makes them distinct from other types of government information and deserving of special precautions that are unnecessary for, say, SEC filings or annual reports. I believe some categories of materials found within PACER do pose special risks and are deserving of special treatment.

Court pleadings are qualitatively different from other types of government records because they are documents created by private citizens engaged in often-heated disputes with their adversaries. They routinely contain sharp and hyperbolic language and make

allegations of fraud, dishonesty, negligence, discrimination, and dereliction of duty. Such allegations, if untrue, would be grounds for defamation suits if made outside of court proceedings. Many cases are dismissed or settled long before the merits of their claims are ever tested before a judge or jury. Yet the allegations linger on in court filings. Unlike court decisions, pleadings are not "the law" but only the raw claims of litigants, untested and unproven. Sitting quietly in the practical obscurity of a court records room or even in the deep Web of the PACER database, such claims are rarely heard by any but the parties to a particular lawsuit. But placed out on the open Web, such claims may never die.

Beyond basic pleadings, other court documents implicate privacy concerns. The courts excluded Social Security litigation from PACER because these claims contain detailed information on the claimants' medical conditions. Many consumer bankruptcies are related to medical expenses and the schedules can reveal significant information about a debtor's medical condition, where a debtor lists doctors and hospitals on the schedule of creditors.

Who's a Rat?

Perhaps the most serious privacy and security concerns arise in criminal cases. One notorious example of abuse of court records is the Who's a Rat Web site (www.whosarat.com). The site claims to have identified 4,300 government informers and 400 undercover agents, many of them from documents obtained from court files available on the Internet. Names and mug shots of the alleged rats are posted on the site, along with plea agreements and other court documents in support of claims that someone is a government informant.

The founders of the site claim First Amendment protection for their efforts. Speaking to ABC News in 2007, Web site spokesman Anthony Capone said, "If people got hurt or killed, it's kind of on them. They knew the dangers of becoming an informant. We'd feel bad, don't get me wrong, but things happen to people. If they decide to become an informant, with or without the Web site, that's a possibility." The same Capone told *The New York Times*, "The reality is this. Everybody has a choice in life about what they want to do for a living. Nobody likes a tattletale." While no deaths have yet been attributed to the Web site, a number of informants have had to be moved into protective custody and some courts have removed plea agreements from the PACER system.

Beyond witness intimidation,

criminal court filings raise other concerns. If a criminal conviction is expunged, it is possible to remove the records from PACER. But if those records have migrated to other databases or to the open Web, the value of expungement is diminished, if not lost. The Electronic Privacy Information Center (EPIC) notes that dissemination of criminal records on the Internet diminishes the chances for social forgiveness, the "principle that one can be born again in America and leave mistakes in the past."

Identity Theft Concerns

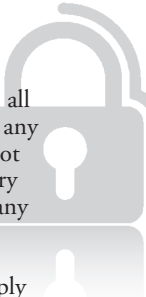
A final concern with all court records, civil and criminal, is the issue of identity theft. The courts have tried to address this by requiring that litigants redact Social Security numbers and other sensitive information from court filings, but compliance has been less than perfect. While some failures to redact private information are no doubt attributable to attorneys, many court documents are filed in hard copy by *pro se* litigants. These documents are scanned into the PACER system by court clerks, and it may not be practical for them to review the documents to ensure no private information is revealed.

Malamud, in reviewing the court records that Swartz downloaded, found numerous instances where litigants failed to redact sensitive information, including one 54-page list of 350 patients of a doctor, complete with names, Social Security numbers, and medical conditions. Malamud has called these lapses to the attention of the courts and Senator Lieberman, and is working to clean up the data he has so that it is free of sensitive private information.

The Demand for Access

Advocates of full and free access to PACER might argue that the genie is already out of the bottle. Perhaps privacy is dead and we should just get over it. Significant portions of the PACER database have been captured by Lexis, Westlaw, and other proprietary databases. Those with access can use the sophisticated search tools in proprietary services to mine data far more effectively than is possible within PACER. Why not provide bulk records to those who wish to develop competing services that are free or cost less than searches in *Wexis*?

Equity of access is the central argument of those who wish to liberate court documents from the confines of PACER. Malamud points out that the data they downloaded "was available to the public, but only in an unjust manner. Any lawyer, identity thieves with cash, or librarians with all-you-can eat Lexis accounts (in short many



millions of people) had full access to all this information, for data mining or any other purpose. The folks that have not had access to the data are the ordinary citizens, scholars, journalists, and many others. Saying that data mining was somehow not happening ignores the reality that this data was public, simply just not evenly distributed.”

Malamud supports rulemaking by the Judicial Conference to better limit the release of sensitive data on PACER, but argues that once a document is public, it needs to be public for all, not just those who can afford to pay.

Finding Balance and Solutions

While some categories of documents within PACER pose special risks to privacy, others do not. The Washington Office of AALL has consistently called for no-fee public access to PACER while also calling for the courts to safeguard private information. Can the courts do both? Below are four recommendations to make the most useful PACER documents freely available on the Web without compromising privacy and security:

- Release all court decisions and briefs in motions and appeals without restriction on the open Internet and make the files available

in bulk to anyone requesting them. These two categories of documents pose little risk to privacy and are among the most used and valuable of the materials in PACER. Exhibits and attachments with private information could be excluded from the release.

- Give attorneys and litigants free and unlimited access to their own dockets. Under the current system, when a new document is uploaded to the court’s electronic docket, parties receive an e-mail notice that allows them one opportunity to download the document to their own computer without charge. While large law firms may capture these documents in sophisticated case management systems, many smaller firms may need to log in to PACER and incur charges to view documents in their own cases. Free access is especially critical for *pro se* litigants, who may not have regular access to computers and need to access PACER repeatedly to view files in their own cases.
- Allow scholars doing empirical research on court records full access to bulk data. The Judicial Conference could establish

reasonable limits on the terms of this access that would protect sensitive data.

- Reinstitute the PACER pilot program and expand the pilot to all federal courthouses. Full release of the database could be prevented by restricting the number of downloads permitted at any one site and instituting reasonable guidelines to prevent abuse. Access should be provided through IP authentication rather than passwords.

Striking the right balance is possible if not easy. PACER has traveled a long way since the days of screechy modems. The next step in the journey is to offer no-fee public access to large portions of the database while still protecting legitimate privacy interests. The AOUSC has stated its commitment to greater access to court records and to protecting privacy. This article’s recommendations are offered with the hope that they will successfully navigate that course. ■

Susan Lyons (slyons@kinoy.rutgers.edu) is documents/reference librarian at Rutgers University Law School Library in Newark, New Jersey.