

Page 1

Privacy and public access to court information has been a major subject of discussion since the advent of the Internet, as evidenced in our good friend and former colleague Susan M. Jennen's book *Privacy and public access to electronic court information: a guide to policy decisions for state courts* published in 1995. The NCSC has continued to monitor information on this subject area and has compiled it [here](#).

But before we get started, please note that this article is not intended to discuss the reasons why or why not access to particular court data should be given to some person or group. But rather it is intended to discuss how access and access control can be technically accomplished.

Picture CCMS12

A Logical Structure to Data Access

The first part of this article focuses on data access by known case participants including judges and court staff. In this scenario we think that the CCMS will be designed to implement multiple design requirements for information access. When designing access one must ask questions. A few of these questions are:

- Who are your information users?
- What information do they want?
- When do they want it?
- How automated and in what format do they want the data?
- How sensitive is your court's data and documents?

The entire Court Technology Bulletin CCMS series will be attempted to build a logical structure that deals with these and other questions. For example, in [Part 3](#) of the CCMS Series we discussed the mapping of the court's organizational structure, the users, and their roles in the court. And in [Part 4](#) we discussed the concepts of Relationships and Groups.

If you can answer the question "who", and have captured that metadata as part of the normal systems operation, you have the ability to create a system with specific access and usage rules for users and groups. And we believe that this design will at least mirror and could very likely result in a better implementation of the statutory and court rule restrictions related to data access.

For example, litigants and their attorneys can be automatically authorized to access all of their documents and information. The system can either provide a case related access pass word or credential for that specific set of data because it knows who is related(grouped) with the case as a participant. And this includes judges, as we recently learned that civil law systems include that as

one of their case information access restrictions.

Extending user identification and thus authorization to access and view information is the big challenge that we have discussed [here](#) and [here](#) before. It can be done. It will take planning and work to achieve. And no, it will not be perfect. No systems, especially including our traditional paper-based systems, are.

The Public Facing Database

First of all, in today's world of almost-free digital storage, and for data security reasons, it makes no sense to expose the court's production case management database on the Internet. Therefore, copies of the production system can be used. And since all of the major commercial databases allow data to be written to two or more instances, this also enables automatic [fail-over](#) /redundancy. But does it make sense for the public version to be the exact copy of the production system? It is now possible to design the systems so that only selected data is automatically copied to the public system. Or the public system could literally be populated using a different technology such as XML that would likely be more useful to data users who don't need event/task production capabilities.

The Commercial Information Industry

In the USA, a huge business has been built around commercial databases of public information. For more than thirty years that we have been working in the courts and visiting courthouses, the commercial data capture business has been something to design for. Courts have had to provide working space, public terminals, and even communications to support. And for more than thirty years we have heard of myriad of problems with the accuracy of the resulting data in the commercial systems.

This is where the political issue of whether or not commercial data firms should be able to use court data at all is often raised. Many courts have adopted a policy often referred to as "practical obscurity" by requiring that data collectors physically come to the courthouse and retype the court information for their purposes.

However even back in the 1990s there was a brief effort to develop a data sharing standard for courts and commercial databases using Electronic Data Interchange (EDI) Technology. EDI was the technical approach used before XML was developed. Two Standards, X12- 175 Court and Law Enforcement Notice and X12-176, Court Submission TYPE were created using the EDI standards. The standards were never widely used but the 176 standard addressed the data to report a "claim disposition or an opinion deciding a case." (see end-notes below)

This approach fixed one of the key problems identified with the practical obscurity approach, the fact that cases often have multiple dispositions such as modifications of judgments/ sentences and, later, sealing, expungement, remanded appeals or pardon. Practical obscurity very often resulted in the data not being captured by commercial providers. This resulted in inaccurate and/or conflicting data about a person that can affect whether or not they can get employment, credit, or housing. Electronic data sharing has become enabled in courts because of technological

advances and pervasiveness of document management systems and E-filing, but their purpose is not primarily public data access. Be aware that the ideal technical approach for public access by sophisticated automated systems is for the court to provide a web service or API interface into the CCMS database as discussed above.

Picture CCMS 13

Identifying the Information Users

Some courts identify data users. This is certainly the case for the US Federal Courts Public Access to Court Electronic Records (PACER) system. But as we were writing this article, one of the technical committees of the OASIS-Open [organization provides some interesting information with the release of the “Identity in the Cloud Use Cases Version 1.0” document \(pdf\)](#). This document [provides a context for development](#) of identity products and services in the future. It is something we will need to monitor as it (hopefully) progresses.

Controlling Data Once it has “Left the System”

Courts are also concerned with data accuracy since errors can revisit as additional cases, procedures, or as bureaucratic headaches. Back in 2005, one of your authors published an [article in the NCSC’s annual Future Trends in State Courts series called, “Digital Rights Management \(DRM\) Technology Will Change the Way Courts Work.”](#) The article explained the basic concepts of how DRM technology works. Of course, since that time many of you have purchased digital music, books, and video from online services that use DRM technology. But courts have not made an investment in it because of the cost and lack of direct financial benefit to create these systems. DRM solves a lot of information issues, [however, so if you are interested we have posted a longer more detailed version of the article online.](#)

Revision #2

Created 8 December 2021 12:54:37 by Niton

Updated 8 December 2021 12:57:18 by Niton