



## Public & Internet Access to Court Records Safety & privacy risks for victims of domestic violence & all citizens using the justice system

### Publishing to the Web versus Public Access

- Publishing highly sensitive family law and victim cases to the web is invasive and unnecessary. The most vulnerable members of our communities may choose not to use the court system for protection or common court services to protect their privacy.
- Court Transparency and Accountability can be achieved by creating non-invasive public search engines that can be put on a court website – allowing anyone to search for trends in types of cases, dispositions, etc... without publishing party names and sensitive details to the world wide web.
- Expensive technology and personnel are needed to redact social security numbers and other information from family and victim court documents. These security and quality assurance measures outweigh potential cost savings for the court.
- Even password protected “subscription” court websites can be linked to one large national search engine and make locating victims easier than ever. Stalkers & batterers will be adept at obtaining subscriptions.
- Sealing a case or filing under a pseudonym may be possible, but difficult in pro se and criminal cases and not sufficient protection for victims.
- There is no public policy purpose of posting victim and witness identities, addresses, and intimate details of DV, SA, and Family Law cases to the Internet. Posting the details of a domestic violence petition or photos from a sexual assault to the web does not support justice and safety for victims.
- Courts should model their policies on ethical privacy practices: including robust notice, choice, accuracy, security, and enforcement – see Fair Information Principles below.

### I. BACKGROUND

State, Local, and Federal Courts are beginning to publish court records to the Internet, providing terminals and kiosks within courthouses, and scanning documents for electronic access. In late 2000, the National Center for State Courts (NCSC) and Justice Management Institute (JMI) began a grant funded project to develop a model policy governing electronic access to court records. The model policy was intended for state systems and local courts to help develop their own policies and guidelines.

The proposed model policy was reframed as “Guidelines” and presented to the Conference of Chief Justices and Conference of State Court Administrators in July 2002 for endorsement. Some state and local courts are planning to adopt the guidelines as such, though the document explicitly outlines complex issues that must be resolved before implementation. The Guidelines are not intended as a template, but rather a discussion guide to help states resolve issues, some which

have life and death implications for victims and other vulnerable citizens in our communities.

The newly termed “Guidelines” have few explicit privacy and safety protections and leave much work to local and state jurisdictions to insure the justice system does not further harm victims & others.

NNEDV has created this paper to help advocates and allies minimize the danger to victims and other citizens when courts are contemplating publishing records and indexes to the Internet.

When courts move beyond allowing paper access to court records, all citizens face increased risk of privacy invasion, identity theft from social security numbers, as well as possible discrimination from allegations in court documents. Victims of domestic violence face possible fatal consequences from common court proceedings such as minor filings and sensitive victim cases becoming web searchable from anywhere in the world.

## II. INCREASED BENEFITS WITHOUT HARMING INDIVIDUALS

Courts can meet their mandate to provide access to public records within the court facility, through paper files or on-site kiosks, without increasing harm and privacy invasions for the most vulnerable citizens in the justice system. The primary purpose of the courts is not to publish stories or sell data. If remote access is desired, it can be done without compromising privacy by developing systems that only allow remote access to the parties in a case.

Court accountability can also be accomplished without harming individual privacy and safety by utilizing internal search engines of summary data, without publishing sensitive identifying case information. For example, a database can provide detailed analysis of numbers, types, and dispositions of cases without compromising the privacy of the individual.

Publishing court records to the Internet is a highly complex endeavor and the quality assurance steps required to insure accurate information can be minimized by not posting family law cases and cases with victims, which usually contain highly sensitive information.

## III. RISKS TO VICTIMS & OTHER CITIZENS

There are many members of the public who have heightened privacy needs in every interaction with the court such as police officers, witnesses in dangerous crime cases, all children, and many others. Victims of all crimes including domestic violence, sexual assault, and stalking should not be further victimized by the very system that purports to help them find safety and justice. Any court system contemplating publishing some case information or case records to the Internet must consider the potential harm to the most vulnerable citizens.

### Existence of a Record on the World Wide Web

The mere existence of a victim's name on a court website could lead a batterer or stalker to a victim's new community, if not exact address. If a victim moves to a new town to start a new life away from a batterer, she might be found if an online court index lists only her name on the Internet. Failing to expressly exclude victim and witness identities from web or remote access will mark these victims and witnesses for continued violence and harassment by the batterer. This encroachment on privacy and the resulting threat to personal safety will discourage victims of domestic violence from seeking protection from their abusers just as it will discourage witnesses from helping to end the violence through their testimony.

Most public filings can give abusers the information they need to track their victims. Posting such filings on the Web increases their utility and accessibility for some, but also increases the chance that victims will be found. For example, if a victim of domestic violence flees her abuser in Virginia, relocates to Texas, buys property, and files her land record with a court that posts such records on the Web, her abuser can find her with a simple, national HTML search. Many of life's most important events involve the court system. In a jurisdiction where the court posts records on the Internet, a victim of domestic violence must weigh the benefits of the activity against the possibility that her attacker will locate her.

### Boston Globe Magazine Cover Story

by Neil Swidey

February 2, 2003

[www.boston.com/globe/magazine/2003/0202/](http://www.boston.com/globe/magazine/2003/0202/)

"Cindy Southworth, director of technology for the National Network to End Domestic Violence, is concerned about the information-on-demand implications for women fleeing abusive relationships. "My biggest fear," she says, "is that it will take a horrific murder - because some court put something on the Web that wasn't supposed to be there - for people to begin taking this seriously."

In the absence of any standardized approach, individual courts nationwide are doing their own thing. One of the courts in the digital vanguard is in Hamilton County, Ohio, where most records are searchable through the court's Web site and, by extension, of course, through Google. I've never met Suzanne or Gregory, but by simply poking around the Hamilton County Web site, I was able to read the full appeals court judgment in their divorce, complete with their salaries and competing child support claims, down to the penny. When I then typed their full names in Google, the same document popped up instantly. Even more distressing to advocates like Southworth: The Montgomery County, Pennsylvania, court posts on its Web site the names and addresses of not just the suspects in abuse cases but the alleged victims as well."

## Inaccurate Information or Publishing a Case to the Web in Error

Inaccurate information published to the web is frequently impossible to correct. The nature of this publishing medium allows search engines (Google, Yahoo, etc) to index information as soon as it is posted to the web. Even if a court corrects a web posting, the inaccurate information may be found by the search engines for all of perpetuity.

There are even archiving sites ([www.archive.org](http://www.archive.org)) that document and preserve websites even if inaccurate information on a court website is removed or corrected in the future.

## Some Records are not Appropriate for Internet Publication

In the past, the content of some court records: health information, details about children, photos of rape victims, and more, would never be published by the courts, and only published by the media if deemed newsworthy and within the bounds of journalism ethics. For this reason alone courts should not publish sensitive case records to the Internet.

Courts must not publish documents relating to civil protection cases to the Internet. In addition, domestic violence cases often spawn divorce proceedings, child custody disputes, and other matters that fall under the larger umbrella of family law.

A court's failure to adequately notify litigants of its information practices would constitute a serious breach of the public trust. The vulnerability of the people it serves and sensitivity of the information it holds only accentuates the courts' duty in this regard. Without robust and clear notice, it is not possible for anyone with heightened privacy needs to make an informed decision whether the court will adequately protect their sensitive information.

It is likely that even most attempts at adequate notice may not reach some of society's most vulnerable members. For immediate safety, victims of violence may feel forced to compromise their long-term privacy and safety needs by using a court that publishes records to the Internet. When courts publish records, adequate notice includes accessible information to assist battered immigrant women, victims with disabilities, and others.

It is entirely likely that the necessary notice will prevent many who desperately need help from using the justice system. Once victims and witnesses learn that the court will publish their information and documents for literally the entire world to see online... they may never use the justice system again.

### An Excerpt from: *Public Records on the Internet: The Privacy Dilemma*

Beth Givens, Director, Privacy Rights Clearinghouse 4/02  
These points are elaborated in the full document at:  
[www.privacyrights.org/ar/onlinepubrecs.htm](http://www.privacyrights.org/ar/onlinepubrecs.htm)

#### NEGATIVE CONSEQUENCES OF ELECTRONIC PUBLIC RECORDS

1. **Less participation in public life.** 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.
2. **Justice only for the rich.** 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. **Identity theft.** The crime of identity theft and other types of fraud will be fueled by easy access to personal identifiers and other personal information via electronic public records. Such information includes Social Security numbers, credit card and bank account numbers, and details about investments.
4. **Destruction of reputations.** Individuals will experience shame and embarrassment, even discrimination, when details of their personal lives are broadcast in court records available on the Internet. The PRC has been contacted by many individuals who have relayed such experiences.

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 because of identity theft. This occurs when an imposter uses an innocent person's identifying information when apprehended by law enforcement. Another scenario is when tax liens and judgments incurred by the identity thief are listed in the name of the innocent victim.

Continued on next page

**CONTINUED Excerpt from: *Public Records on the Internet: The Privacy Dilemma***

5. **Personal safety risks.** Victims and witnesses who are named in court records could be put at risk. The personal safety of victims of domestic violence and stalking, for example, could be jeopardized. A domestic violence expert who contacted the PRC told me that many victims of stalking and domestic violence do not file cases in court because they do not want their private information being in the public arena for fear of it being used by the stalker to locate and harm them. Witnesses to crimes could also be put in harm's way because of retribution from the perpetrators and other parties to the crimes.
6. **Secondary uses of information.** 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.
7. **Dossier society.** 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.
8. **Loss of social forgiveness.** 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."
9. **Growing numbers of disenfranchised individuals.** 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.

"Computer databases contribute significantly to what I call the "aggregation problem." The aggregation problem stems from the fact that the digital revolution has enabled information to be easily amassed together. We often sprinkle small details about ourselves in a variety of settings as we go about our daily lives. .... But imagine if every person or entity we ever came into contact with during our lives pooled everything that they knew about us. A fact here and a detail there add up." (p.14)

Law professor Daniel Solove ("Access and Aggregation: Public Records, Privacy, and the Constitution," 8/10/2001

[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=283924](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=283924), & in the *Minnesota Law Review*, Vol. 86, No. 6, 2002.)

### III. SAFER SOLUTIONS

#### A. Exclude documents in civil protection matters, family law, domestic violence, sexual assault, and stalking cases from remote or Internet access

- Public vs Published. A court may consider these cases "public" and provide access at a court facility without "publishing" them to the web.
- People who have a need to look at these cases can come into the courthouse for onsite paper or electronic access.
- We do not want young children learning how to search the Internet in school to find their own custody or parent's divorce petitions and allegations on the Internet.
- These cases do not create high volume access in the courthouse such as a large civil class action case that might have many plaintiffs and attorneys wanting remote or Internet access to reduce time at the courthouse. There is a higher likelihood that remote or Internet access would make it more convenient for people misusing this information.

**B. Exclude domestic violence & sexual assault victim and witness identities from any public access and online remote access**

- Restrict contact information categorically (home address, phone, email) from any public access if at all possible.
- Restrict remote/Internet access to names in domestic violence, sexual assault, stalking, family law, & protection order cases.
- Allow individuals to restrict access to their names in docket listings (since many docket listings are shared widely and being posted to the web).

**C. Apply the access principles to all records maintained by the court including non-court records housed in the courthouse**

- The Model Guidelines only apply to judicial case records, not all records maintained by court (marriage licenses, land records, etc) however some courts may automatically move to post all records housed by the courts on the Internet. A victim may relocate and need a common record filed at the court – if the land title is posted to the Internet, it will be easily searchable.
- The executive branch may be responsible for non-judicial records housed in a courthouse (land records, etc). Communities should work with all branches of government to categorically or case-by-case prevent Internet publication.

**D. Prevent the disclosure of protected information in web based summary documents or indexes**

- Anyone should be able to petition to restrict access in a variety of ways: file under initials or pseudonym, restrict remote or onsite access to a case -- docket number could be listed with no name and a note “case restricted or sealed”, etc.
- Many court systems are posting to the Internet their docket lists with summary information including name, address, docket number, case disposition, and other summary data. An online docket listing could put a victim at risk of being located by a batterer or stalker.

**E. Allow any petitioner to exclude all court records from remote access**

- Any citizen should be able to petition the court to restrict access in a variety of ways: file under initials or pseudonym, restrict remote or onsite access to a case -- docket number could be listed with no name and a note “case restricted or sealed”, only summary information on the web not the actual documents, etc.
- Many citizens including survivors of domestic violence, sexual assault, and stalking may have legitimate concerns about their information being posted by the courts to the Internet. Since the court can choose to provide access within the courthouse, anyone should be able to petition the court to restrict remote access. Since this is not the same as sealing a case completely, a lower standard may apply. (Consult an attorney in your state for legal advice).

**F. Information must be protected from the time of request through decision of the court**

- If someone petitions the court to either completely seal a case or restrict remote/Internet access (see D. above) their case and all information about it should be protected from the time of the request until a decision is made.
- If the court posts a case to the web while the request to restrict Internet access is pending review, then a victim’s privacy and safety could be violated. If there is no protection of the information while a request is being reviewed, than many victims may need to choose to NOT USE THE COURT – for anything.

**G. If a court denies a request to seal or restrict remote/Internet access, a victim must be able to remove her court documents without her papers being posted to the Internet. In some cases, victims might have to choose safety and privacy over using the court system.**

- If a petition to restrict Internet publication is denied, then a victim must have the ability to withdraw her initial filing without her petition to withdraw being posted to the web.

## **H. Permit local courts to adopt more restrictive access policies than the National Model “Guidelines”**

- The February 2002 proposed Model Policy encouraged states to prohibit local courts from having more restrictive access policies than the state uniformly adopts. This is counterproductive in a state where the uniform policy is harmful to victims and a local court is receptive to protecting victim information.
- Local courts should have the latitude to protect the privacy and safety of their constituents. State courts might want to set a minimum level of privacy so that local courts don't post too much information to the Internet, but should not tell local courts that they must post as much private data as a less conscientious court jurisdiction.

## **I. Provide robust notification of electronic record management to litigants, victims, witnesses, and the community, including victim advocacy groups**

- Any court contemplating increasing access to court records MUST provide robust notice on where the records are posted AND also how to restrict access. Many comparable data privacy doctrines require comprehensive notice.
- Some court staff may be hesitant to include notice on how to restrict access for fear that a) all who use the court will petition for restriction and b) witnesses and victims might not participate in hearings if they understand that information about them will be posted to the Internet. This concern is never a valid reason for limited notice.
- Clear signs posted throughout the courthouse could assist in this notice, as could a brochure to give to witnesses when they are called to the court since frequently court administrators do not know witness identities prior to a hearing. Other officers of the court (prosecutors, etc) can also provide comprehensive notice to victims and witnesses.
- Courts should work with local and state victim advocacy groups if they are contemplating increasing access to sensitive court records and data through the Internet or other electronic means. State coalitions and local programs can assist victims in navigating the petitions to restrict access and planning for safety about potential

consequences of using court systems that post victim data.

- Also, notice for pro se litigants is critical. There are many pro se litigants without attorneys to explain the courts publication policy. All victims, witnesses, and pro se litigants need effective notice.

## **J. Include processes for preventing and remedying failures to properly exclude information from public access**

- All good technology initiatives include quality assurance and auditing processes. Courts must include a comprehensive and timely process PRIOR to posting any court records into an electronic system connected to the Web.
- Preferably, an outside neutral office should assist or oversee an audit process to check for errors. Random sampling of all cases and checking cases where restrictions to access were granted would help identify if the court is posting information to the Internet in error. State Courts could oversee an audit process of local courts. Alternatively or in addition, an office in the court that is not responsible for the day-to-day management of the electronic court records could oversee an audit.
- Since it can be assumed that errors will occur, a timely remedy process should be developed prior to implementing an electronic system. Depending on the nature of the error (posted a case to the Internet that was not supposed to be posted at all or an error within a court document) the court might want judicial review – however it should be timely. Victim safety and citizen privacy could be compromised by an error and due to Internet Search engines, selling court data in bulk, and Internet Archives, time is of the essence.
- All court staff including judges should be required to participate in training on any electronic system to reduce errors and assist in granting petitioners appropriate restrictions on Internet publication. All court staff should know the process to request a restriction of access and also the process to remedy an error, even if that process is the correct referral to the appropriate staff person.

## Fair Information Principles

A set of fair information principles have emerged as the model for much existing and proposed privacy legislation. These principles -- notice, choice, access, security, and enforcement – are the accepted standard for building effective privacy policies.

The below summary is excerpted from the **Privacy Journal** website: [www.privacyjournal.net/bio.htm](http://www.privacyjournal.net/bio.htm)

1. Organizations establishing privacy policies should incorporate the elements of the widely accepted \*Code of Fair Information Practice:
  - The existence of all data systems with personal information in them should be publicly disclosed, and the purpose for which information is gathered about people should be disclosed. This is the principle of openness or transparency.
  - There must be a way for an individual to find out what information about him or her is in a record and how it is used.
  - There must be a way for an individual to prevent information about him or her that was obtained for one purpose (which was stated when the information was gathered) from being used or made available, either within the organization or outside, for a purpose that is incompatible with the original purpose, without getting the consent of the individual. This is the principle of secondary use.
  - There must be a way for an individual to correct or amend a record that contains information that is identifiable to him or her.
  - The organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability, accuracy, security and timeliness of the data. In other words, the custodian of information that is disseminated has an obligation to the individual to make sure it is accurate, secure, and not misused. This obligation ought not be delegated to another entity.
2. An organization must make sure that other entities handling personal information in behalf of the first organization are bound by these same principles.
3. An organization must conduct periodic risk assessments, balancing the possibility or probability of unauthorized access or disclosure against the cost of security precautions and the expected effectiveness of the precautions. In some cases, it will be necessary to establish an audit trail so that records are kept of disclosures of personal information, both within the organization and outside.
4. Organizations must take special precautions in collecting and using personal information about children, both those 13 or younger and those 18 or younger.
5. An organization should openly disclose its policies and practices with regard to electronic surveillance of its employees' and customers' telephone calls, electronic mail, Internet usage, changing rooms, and rest rooms. It must articulate in advance the reasons for the surveillance.
6. An organization should collect only that personal information that is PROPORTIONAL to the purpose of the information. It must scrutinize each demand for information to determine that it is relevant and necessary.
7. An organization should designate an individual or office (whether full-time or part-time) to handle privacy issues by (a) acting as an ombudsman for customers or employees, (b) assessing the privacy impact of new undertakings, (c) assuring that the organization complies with all laws and trade-association standards; and (d) informing the organization of the latest technology and policies that affect the privacy of customers or employees. An organization, if it utilizes "opt-out" for customers to stay out of certain uses of their information, should make exercising "opt-out" easy, as easy as clicking a button or checking a box, without the need to write a letter or to communicate with another office.
8. An organization should conduct periodic training of its employees (and volunteers) to assure that they know (1) applicable laws on confidentiality that govern the organization, (2) the organization's policies and actual practices, (3) the rationale for protecting confidentiality and the sensitivity of personal information, (4) the ability to recognize possible breaches and to report them to the proper person. An organization may chose to certify that employees who handle personal information are properly trained.

\*The Code of Fair Information Practice was first established by the U.S. Department of Health, Education, and Welfare's report on RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS (1973) and ratified by a similar study by IBM Corp. The Business Roundtable in the U.S. endorsed the code in the 1970s and it became a part of all data protection laws in Europe and most of the privacy laws in the U.S.

## APPENDIX 1: ADDITION RESOURCES & ARTICLES

1. **The National Network to End Domestic Violence** [www.nnedv.org](http://www.nnedv.org)  
660 Pennsylvania Ave SE, Suite 303, Washington, DC 20003 202-543-5566

2. **A Nation of Voyeurs:** How the Internet search engine Google is changing what we can find out about one another - and raising questions about whether we should **By Neil Swidey, Globe Staff, 2/2/2003**  
[www.boston.com/globe/magazine/2003/0202/coverstory.htm](http://www.boston.com/globe/magazine/2003/0202/coverstory.htm)

3. **Articles by Professor Daniel J. Solove:**  
[http://law.shu.edu/faculty/fulltime\\_faculty/soloveda/solove.html](http://law.shu.edu/faculty/fulltime_faculty/soloveda/solove.html)

- Identity Theft, Privacy, and the Architecture of Vulnerability  
54 Hastings Law Journal (2003)  
[www.law.berkeley.edu/cenpro/samuelson/eprs/papers/solove-privacy-vulnerability.pdf](http://www.law.berkeley.edu/cenpro/samuelson/eprs/papers/solove-privacy-vulnerability.pdf)
- Digital Dossiers and the Dissipation of Fourth Amendment Privacy  
75 Southern California Law Review 1083 (2002)  
[http://law.shu.edu/faculty/fulltime\\_faculty/soloveda/digital\\_dossiers.pdf](http://law.shu.edu/faculty/fulltime_faculty/soloveda/digital_dossiers.pdf)
- Conceptualizing Privacy 90 California Law Review 1087 (2002)  
[http://law.shu.edu/faculty/fulltime\\_faculty/soloveda/concept\\_privacy.pdf](http://law.shu.edu/faculty/fulltime_faculty/soloveda/concept_privacy.pdf)
- Access and Aggregation: Public Records, Privacy, and the Constitution  
86 Minnesota Law Review 1137 (2002)  
[http://law.shu.edu/faculty/fulltime\\_faculty/soloveda/access\\_aggregation.pdf](http://law.shu.edu/faculty/fulltime_faculty/soloveda/access_aggregation.pdf)
- Privacy and Power: Computer Databases and Metaphors for Information Privacy  
53 Stanford Law Review 1393 (2001)  
[http://law.shu.edu/faculty/fulltime\\_faculty/soloveda/kafka\\_orwell\\_privacy.pdf](http://law.shu.edu/faculty/fulltime_faculty/soloveda/kafka_orwell_privacy.pdf)

4. **Code of Fair Information Practice** <http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm>

5. **Electronic Privacy Information Center** [www.epic.org/](http://www.epic.org/)

6. **Federal Trade Commission: privacy policies** [www.ftc.gov/privacy/index.html](http://www.ftc.gov/privacy/index.html)

7. **Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems** <http://www.ncja.org/pdf/privacyguideline.pdf>

Some privacy issues can be addressed through basic tenets of information collection and use and the *Guideline* provides specific direction on how to employ good collection and use practices. The *Guideline* also discusses a number of other privacy issues that are not as clearly solved from agency to agency or jurisdiction to jurisdiction, such as determining the sensitivity or public accessibility of certain data. The *Guideline* was prepared through a national and international collaboration of nearly 100 state, local and tribal justice leaders, as well as academia, elected officials, the media and the commercial sector. We invite you to copy and distribute this document freely to all who are interested and to those who should be informed about issues concerning privacy in justice information systems.

8. **Privacy Journal** [www.privacyjournal.net](http://www.privacyjournal.net)

9. **Privacy Rights Clearinghouse** [www.privacyrights.org/](http://www.privacyrights.org/)

## APPENDIX 2: DISCOVER WHAT IS HAPPENING IN YOUR COMMUNITY

### \* Some courts are currently publishing victim information or records to the Internet.

Some communities are publishing all court records to the Internet already. Other court systems are working towards that goal. Some courts have intentionally decided against posting certain cases and information on the Internet. After reconsideration, some courts have removed protection order case information and victim information from their court websites. Under national criticism and scrutiny, a county in Pennsylvania is reconsidering their decision to post victim names and addresses in protection order cases, with no notice or recourse for these vulnerable parties.

### Some suggested strategies to discover how court records are accessed and published

- **Ask your local court** administrator, clerk of courts, or ally in the court system if records can be accessed via the Internet, dial-in computer systems, public kiosks in the courthouse, etc.
- **Ask your state court administrator** (Administrative Office of the Courts or AOC in many states) – many state court administrative offices have a technology person or division. They may know which local courts have online access to court records and which courts are moving towards online access.

<http://cosca.ncsc.dni.us/> **The Conference of State Court Administrators (COSCA)** has a Member Directory which might list a contact person in your state.

- **Search on the Internet** for a Local or State Court website. [www.google.com](http://www.google.com) is a popular search “engine” as is [www.yahoo.com](http://www.yahoo.com). Type the name of your county/state & the word “court”  
[www.ncsconline.org/D\\_KIS/info\\_court\\_web\\_sites.html#state](http://www.ncsconline.org/D_KIS/info_court_web_sites.html#state) The National Center for State Courts has a listing of **State Court Web Sites** that includes many local and municipal court Web sites.
- **Go into your local courthouse** and use a kiosk, terminal, &/or paper system to see if victim names, addresses, petitions, etc are easily searchable by any member of the public. One advocate discovered a form given by the court administrator to victims titled “confidential” requesting contact information of the victim was being stored in the public civil record – for the defendant or his attorney or anyone to read. Once alerted, the court administrator stopped storing this form in the public civil record.
- Look for existing or pending **local or state rules, policies, or legislation**.