The Honorable Brook Hedge
Chair, Technology Committee

The Honorable Anita Josey-Herring
Presiding Judge, Family Court

The Honorable Linda Turner
Presiding Judge, Domestic Violence Unit

District of Columbia Superior Court
500 Indiana Ave., N.W.
Washington, D.C. 20001

October 19, 2007

Re: Comments of District of Columbia Domestic Violence and Privacy Advocates on Online Remote Access to Case Dockets.

We are responding to your request for comments on the development of a policy for remote access to court docket information. At a September 19th Courthouse Meeting entitled "Confidentiality v. Convenience: Should Domestic Violence and Domestic Relations Cases Be on the Court's Website," you asked for our comments on online remote access to those dockets. You also asked that we prepare a proposed policy.

The Violence Against Women Act ("VAWA") sets minimum privacy requirements with which the Court must comply, and specifically prohibits publication of information currently contained within several court dockets.[1] Additionally, domestic violence survivors also experience privacy risks from the public availability of court records not covered under VAWA. The principles of Fair Information Practices are a well established expression of the minimum interests that have guided information privacy policy for over 30 years. We present a proposed policy that meets VAWA's legal requirements, follows established Fair Information Practices, and includes convenience, oversight and transparency.

We stress that the Court should place records online only once it has the resources and technical ability to implement these appropriate privacy protections.

I. VAWA PROHIBITS THE INTERNET PUBLICATION OF KEY PROTECTION ORDER INFORMATION

[1] Violence Against Women and Department of Justice Reauthorization Act, P.L. No. 109-162, 119 Stat. 2959 (2005) [hereinafter VAWA 2005].

In 2005 Congress reauthorized the Violence Against Women Act.[2] VAWA includes key provisions related to privacy.[3] VAWA was updated to contain restrictions on the Internet publication of certain protection order information.

a. Petitioner's "Location" and "Identity" Must be Protected.

VAWA 2005 prohibits the Internet publication of the identity and location of protected persons:

> c) Limits on Internet Publication of Protection Order Information.--Section 2265(d) of title 18, United States Code, is amended by adding at the end the following:
> "(3) Limits on internet publication of registration information.--A State, Indian tribe, or territory shall not make available publicly on the Internet any information regarding the registration or filing of a protection order, restraining order, or injunction in either the issuing or enforcing State, tribal or territorial jurisdiction, if such publication would be likely to publicly reveal the identity or location of the party protected under such order. A State, Indian tribe, or territory may share court-generated and law enforcement-generated information contained in secure, governmental registries for protection order enforcement purposes."[4]

VAWA defines "protection order":

> (20) Protection order or restraining order.--The term 'protection order' or `restraining order' includes--
> (A) any injunction, restraining order, or any other order issued by a civil or criminal court for the purpose of preventing violent or threatening acts or harassment against, sexual violence or contact or communication with or physical proximity to, another person, including any temporary or final orders issued by civil or criminal courts whether obtained by filing an independent action or as a *pendente lite* order in another proceeding so long as any civil order was issued in response to a complaint, petition, or motion filed by or on behalf of a person seeking protection; and
> (B) any support, child custody or visitation provisions, orders, remedies, or relief issued as part of a protection order, restraining order, or stay away injunction pursuant to State, tribal, territorial, or local law authorizing the issuance of protection orders, restraining orders, or injunctions for the protection of victims of domestic violence, dating violence, sexual assault, or stalking.[5]

VAWA prohibits the publication of information that is "likely to publicly reveal the

[2] *Id.*
[3] *See* VAWA and Privacy, http://www.epic.org/privacy/dv/vawa.html.
[4] VAWA 2005, *supra* note 1, at § 106, 119 Stat. 2982.
[5] *Id.* at § 3, 119 Stat. 2966-67.

identity or location" of the petitioner. The prohibition extends to more than just the petitioner's name and address data fields in a docket. The respondent's name may be "likely to reveal" the identity of the petitioner because they are necessarily in an intrafamily relationship.[6] Noting that an un-named petitioner is the spouse of a named respondent is quite "likely to reveal" the identity of the petitioner.

Further, the docket entry reveals the location of the petitioner as being the District of Columbia. This is a significant risk as an out of state protection order registered in the District will reveal that the protected person has relocated to or has ties to the District.

b. Several Court Dockets Contain Information Prohibited From Publication.

The VAWA limitation reaches several of the Superior Court Dockets. Furthermore, the VAWA language also affects the unredacted publication of D.C. Court of Appeals cases involving protection order information.

VAWA Prohibits Online Publication of the Civil Protection Order (CPO) Docket. The Civil Protection Order Docket contains cases filed pursuant to the Intrafamily Offenses Act. It is extremely unlikely that a case in the CPO docket will not qualify as a "protection order" for the purposes of the VAWA Internet publication prohibition. Part A of the VAWA "protection order" definition covers orders prohibiting further abuse and contact, as well as "stay away" orders, for all individuals.[7] Part B of the VAWA "protection order" definition covers child custody and support provisions when issued as part of a protection order for victims of domestic violence, dating violence, sexual assault or stalking.[8] Civil Protection Orders provide for petitioners several forms of relief: freedom from harassment; that the respondent stay away from petitioner; that the respondent not contact petitioner; awarding of temporary legal and physical custody; awarding of rental or mortgage assistance payments; and other relief.[9] It will be unlikely that an order is filed which does not fit into either category.

VAWA Prohibits Publication of Protection Order Information in the Domestic Relations (DR) Docket. The domestic relations docket will contain protection order information when these are consolidated with other matters concerning the same family.[10] Even if only the existence or case number of a CPO is noted, this notation is "likely to publicly reveal the identity or location" of the protected person because this

[6] D.C. CODE ANN. § 16-1005(c)(2007).

[7] VAWA 2005, *supra* note 1, at § 106, 119 Stat. 2982.

[8] *Id.*

[9] D.C. CODE ANN. § 16-1005(c)(2007).

[10] DC CODE ANN. § 16-1004(a) (2007) ("Upon a filing of a petition for civil protection by the Attorney General or by a complainant, the Family Division shall set the matter for hearing, consolidating it, where appropriate, with other matters before the Family Division involving members of the same family").

person will be one of the parties to the domestic relations case. Therefore the notation of a protection order in a domestic relations case published on the Internet violates the VAWA prohibition.

The DR docket will also contain injunctions against violence in divorce and custody cases. These injunctions qualify as a "protection order" under VAWA if any civil order was issued in response to a complaint, petition or motion made by or on behalf of the protected party. Thus their publication is prohibited if they are "likely to publicly reveal the identity or location" of the protected party.

VAWA Prohibits Publication of Protection Orders in, and Certain Information From, the Criminal (DVM, FEL) Dockets. Criminal cases that are associated with a CPO are also barred from Internet publication if the publication includes any information from the CPO that fits the VAWA definition. Listing a complaining witness would be prohibited when that witness is the protected person. Further, the identity of the defendant or of an unprotected complaining witness may be "likely to reveal the identity and location" of the protected person.

Even if no CPO is listed, a stay away order in a criminal disposition may qualify as a "protection order" for VAWA purposes if an unlisted CPO existed. Per section A of the VAWA definition, a criminal stay away would qualify "so long as any civil order was issued in response to a complaint, petition, or motion filed by or on behalf of a person seeking protection." A stay away order identifying the protected individual would reveal the identity of a protected person. A stay away order providing an address or location would likely reveal the location of the protected person.

VAWA Prohibits Publication of Civil Restraining Orders in the Civil (CV) Docket. The VAWA prohibition is not limited to the Intrafamily Offenses Act's limitation of jurisdiction to those cases where there is an intrafamily relationship.[11] Petitioners who do not meet this definition must file for a civil restraining order in the civil docket. Thus a civil restraining order issued pursuant to D.C. SCR-Civil Rule 65 will qualify for the VAWA limitation if it has the "purpose of preventing violent or threatening acts or harassment against, sexual violence or contact or communication with or physical proximity to" the petitioner.

II. DOMESTIC VIOLENCE SURVIVORS FACE PRIVACY RISKS FROM ALL SECTIONS OF THE COURT DOCKET

Domestic violence survivors have privacy interests and face privacy risks in all the public records that the Court maintains. The VAWA provisions only reach records related to protection orders. Nonetheless, the Court should protect other records as well.

These risks are examples of how the very purposes of public records -- citizen

[11] D.C. CODE ANN. § 16-1001(5)(2007).

oversight and transparency -- are turned on their heads when records contain excessive information and are disseminated without adequate privacy protections. Instead of being a system via which citizens keep tabs on their government, records become a means by which government, data brokers and others pry into the lives of individuals.

Currently, for those dockets the Court places online, the only method of avoiding the Internet publication of a docket record is to originally file the case under seal. The choice has to be made at the time of filing by the petitioner / plaintiff, and they cannot later try to remove the case from Internet publication. Further, a defendant / respondent has no choice in the matter, even if he or she is the actual domestic violence victim and the filing is a result of retaliation by the abuser.

a. The mere existence of a record on a website leads a batterer to a survivor's new community.

The existence of a docket entry containing any information about a domestic violence survivor on the Internet may indicate that the individual is in the District. This leads an abuser / stalker to knowing that the individual is in the District. Even more detail may be present, as some docket entries contain address information for where individuals are served. A landlord tenant dispute, or a collections matter, will typically expose an individual's address on the Internet.

b. Mere existence of domestic violence or domestic relations records lead to reputation harms.

Employers, landlords and other community members hold prejudicial views of those involved in domestic violence. Some blame the victim, or attach some form of stigma to them. An employer may feel that their workplace is threatened, or that the victim will be unable to work satisfactorily. A landlord may feel that the victim will be unable to pay rent, or maintain the property in good condition. These individuals may not even know the difference between a "petitioner" and "respondent." Landlords are prohibited from discriminating based upon one's status as victim of an intrafamily offense.[12] Protecting the privacy of this information aids the public policy prohibiting this discrimination.

In the domestic relations docket, docket entries will include rulings for home studies and mental health evaluations. This information will also cause reputation harms if widely available.

As discussed in section IV below, these records will not only be available from the Court website. Increasing online access will increase the dispersion of records to third party information brokers. Thus the stigma attached to individuals by virtue of these records will spread.

[12] D.C. Code Ann. § 2-1402.21 (2007).

c. Fear of a loss of privacy may cause less participation in public life as individuals avoid the creation of public records.

The privacy threats discussed throughout these comments may dissuade individuals from filing legitimate cases whether domestic violence related or not. Thus they will be dissuaded from using the Court and dissuaded in participating in the justice system. In contrast, wealthy individuals will have access to more expensive private mediation services. These do not raise the privacy issues that court records raise. The result will be an unequal access to justice.

d. Identity theft is facilitated by making personally identifiable information available online.

Remote access facilitates identity theft by providing identity information at a low cost to the Internet at large. Ten years ago, Maricopa County in Arizona began a policy of placing large numbers of public records online.[13] They now have one of the nation's highest rates of identity theft. Records placed online by a court in Ohio was a source of identity information for a ring of identity thieves.[14] Participants in the Court system should not have their records exposed to identity thieves.

e. Court records are subject to secondary uses unrelated to the litigation or oversight purpose of their publication.

These records are used by data brokers for marketing and profiling. Harmful stigmatization may also result as employers, landlords, creditors and others may hold inaccurate beliefs about the domestic violence survivor's ability to work, pay the rent or cover other bills. Social stigma is also a risk, as some hold inaccurate beliefs about domestic violence survivors, such that they are at fault for their abuse.

III. WELL ESTABLISHED PRIVACY PRACTICES SHOULD GUIDE COURT POLICY

Fair Information Practices establish minimum standards for handling personally identifiable information. Fair Information Practices were first developed in 1973 by the U.S. Department of Health Education and Welfare's (HEW) Advisory Committee on Automated Personal Data Systems.[15] The Committee was set up "in response to the

[13] CIO.com, Country Rife With Identity Theft Reconsiders Online Records (Dec. 22, 2005), http://www.cio.com/article/16011/County_Rife_with_Identity_Theft_Reconsiders_Online_Records

[14] Lisa Myers, Online Public Records Facilitate ID Theft, MSNBC, Feb. 5 2007, http://www.msnbc.msn.com/id/16813496/.

[15] U.S. Department of Health, Education and Welfare, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, 41-42 (1973).

growing concern about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage and use of data about individual citizens."[16] The report concluded that "the net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems." In order to achieve a balance, they proposed the ideas of openness; individual participation, security and reliability, and use limitations.[17]

The principles have been reformulated and have gained international acceptance. In 1980, the Organization for Economic Cooperation and Development published a set of 8 principles[18]:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:
   a) with the consent of the data subject; or
   b) by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle: An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

[16] *Id.* at viii.

[17] *Id.* at 41-42.

[18] Organization for Economic Security and Co-Operation, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

b) to have communicated to him, data relating to him
   - within a reasonable time;
   - at a charge, if any, that is not excessive;
   - in a reasonable manner; and
   - in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

The Electronic Privacy Information Center (EPIC) has previously made specific recommendations on court records. In comments to the Pennsylvania courts, EPIC noted that minimization, and access and use limitations were key to privacy protection.[19] In comments to the Florida courts, EPIC again recommended minimization, limiting acceptable re-uses, and limiting the appearance of unique identifiers.[20]

IV. DATA MINERS' ABUSIVE PRIVACY HARMS SHOULD NOT BE FACILITATED

In the past, privacy interests in public records were protected by the rule of "practical obscurity." The cost and time involved in getting a paper record from a court clerk with an actual site visit effectively protected the record. Now, data brokers access these public records, enter them into electronic format outside of the control of courts, and commodify them. Courts that facilitate access with technology will see more of their records captured. Likewise, courts that do not place limits on re-uses of records will see brokers distribute information about their citizens.

The privacy risks identified in section II are magnified by these data broker products. Data brokers increase the spread of records. Brokers also combine these records with other information sources, building profiles on individuals.[21] Furthermore, they make correction harder, and reliability lower: as information disseminates to several databases, an update in the original may not follow to the further records. Brokers also decrease the Court and subject's ability to control the integrity of records: a record that is expunged or sealed cannot be removed from the broker's database, even if it will be

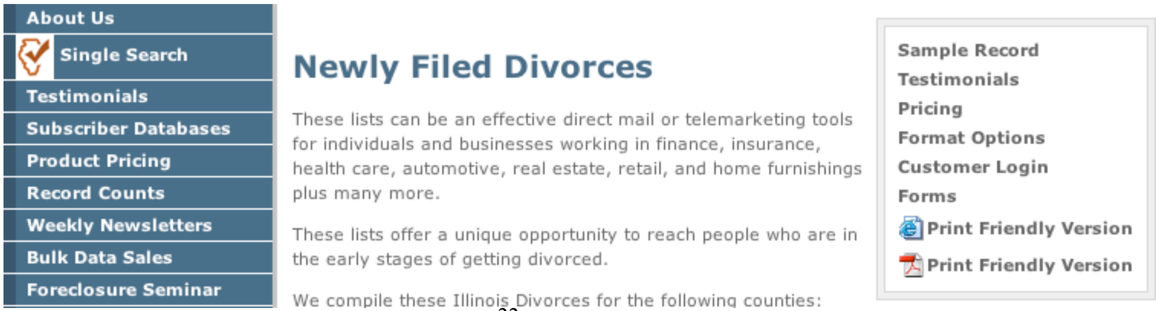
[19] Electronic Privacy Information Center, *Comments on Privacy and Access to Court Records* (Nov. 9, 2005), *available at* http://www.epic.org/privacy/publicrecords/paecfcomments.html.

[20] Electronic Privacy Information Center, *Comments to the Committee on Privacy and Court Records* 12-13 (Nov. 1, 2004), *available at* http://www.epic.org/privacy/publicrecords/flcomments.pdf.

[21] *See* EPIC Privacy and Public Records Page, http://www.epic.org/privacy/publicrecords/,

removed from public viewing by the Court. Likewise, a record that is corrected by the Court is not guaranteed to be corrected by a third party data broker.

Data Brokers do not access data for purposes of litigant convenience, transparency in government or oversight. Their purposes are commodification, commercial resale, and profiling. Several examples of these commercial services are provided:



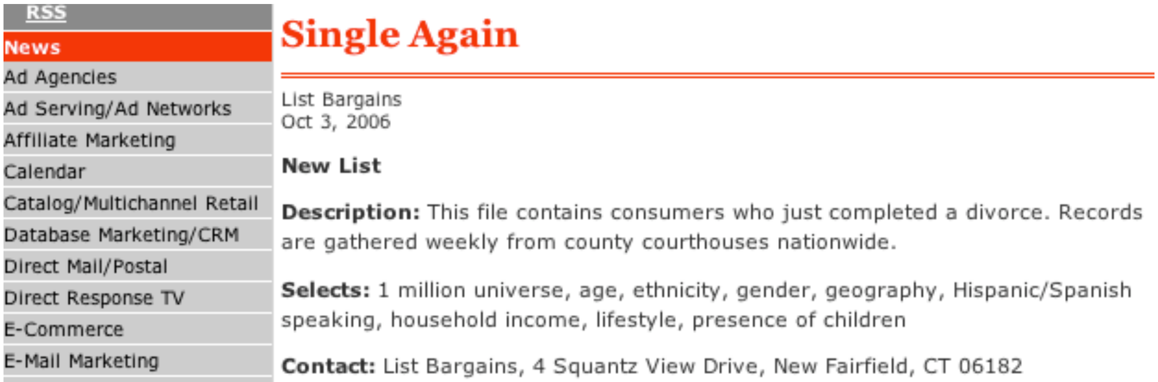
Newly Filed Divorces

These lists can be an effective direct mail or telemarketing tools for individuals and businesses working in finance, insurance, health care, automotive, real estate, retail, and home furnishings plus many more.

These lists offer a unique opportunity to reach people who are in the early stages of getting divorced.

We compile these Illinois Divorces for the following counties:

(Source: Record Information Services.[22])



Single Again

List Bargains
Oct 3, 2006

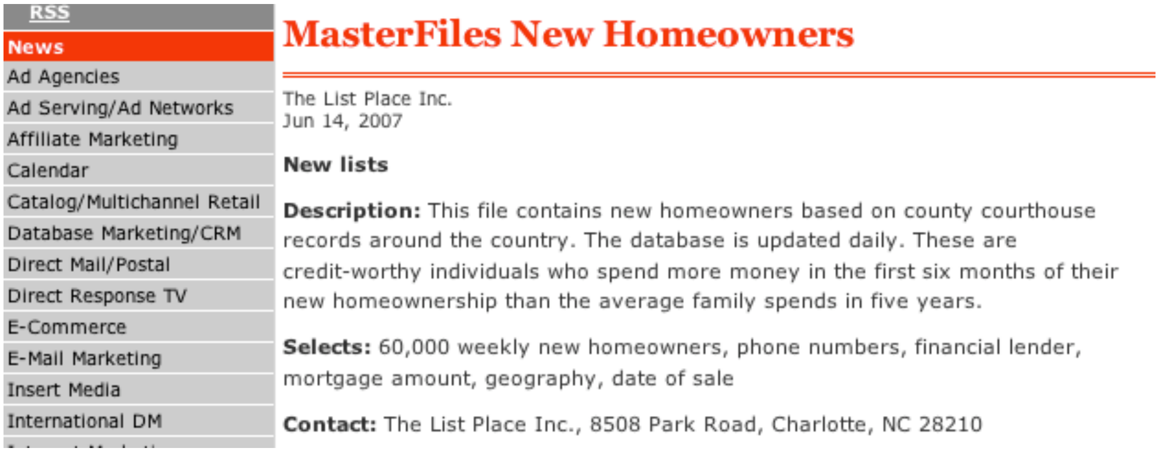
New List

Description: This file contains consumers who just completed a divorce. Records are gathered weekly from county courthouses nationwide.

Selects: 1 million universe, age, ethnicity, gender, geography, Hispanic/Spanish speaking, household income, lifestyle, presence of children

Contact: List Bargains, 4 Squantz View Drive, New Fairfield, CT 06182

(Source: Direct Marketing News.[23])



MasterFiles New Homeowners

The List Place Inc.
Jun 14, 2007

New lists

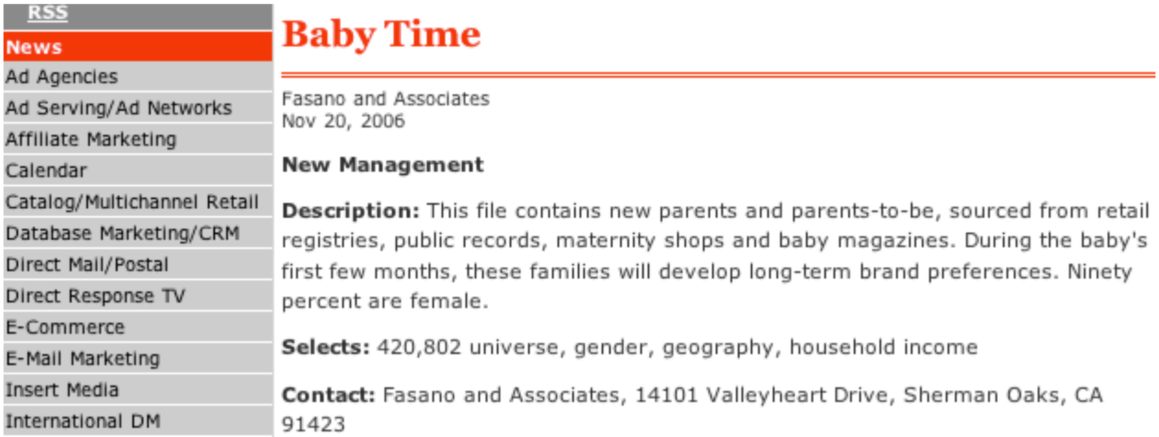
Description: This file contains new homeowners based on county courthouse records around the country. The database is updated daily. These are credit-worthy individuals who spend more money in the first six months of their new homeownership than the average family spends in five years.

Selects: 60,000 weekly new homeowners, phone numbers, financial lender, mortgage amount, geography, date of sale

Contact: The List Place Inc., 8508 Park Road, Charlotte, NC 28210

[22] http://www.public-record.com/content/databases/divorces/index.asp
[23] http://www.dmnews.com/list/449.html.

(Source: Direct Marketing News.[24])



Baby Time

Fasano and Associates
Nov 20, 2006

New Management

Description: This file contains new parents and parents-to-be, sourced from retail registries, public records, maternity shops and baby magazines. During the baby's first few months, these families will develop long-term brand preferences. Ninety percent are female.

Selects: 420,802 universe, gender, geography, household income

Contact: Fasano and Associates, 14101 Valleyheart Drive, Sherman Oaks, CA 91423

(Source: Direct Marketing News.[25])

These lists are not just used for intrusive and annoying marketing and profiling. They are also used by predatory entities worldwide to target individuals for criminal purposes. Data Broker InfoUsa sold lists of elderly individuals it advertised as "gullible."[26] Telemarketing fraudsters used these lists to prey on those individuals and steal from their bank accounts.[27]

V. TECHNICAL AND LEGAL MEASURES SHOULD PROTECT INFORMATION FROM DATA BROKERS.

The Court should take care not to facilitate these data broker activities in the interest of convenience and oversight. Lowering the cost of acquiring data lowers the prices data brokers charge when they make it available. This in turn increases its distribution. The rule of "practical obscurity" -- which protected the privacy of paper records -- still exists as a continuum of cost. Records lose their obscurity as the Court facilitates data broker access.

Remote access systems should be technically configured to avoid data brokers. Major search engines respect the directions of a website that delineates which sections can and cannot be searched. As the Official Google Blog explains:

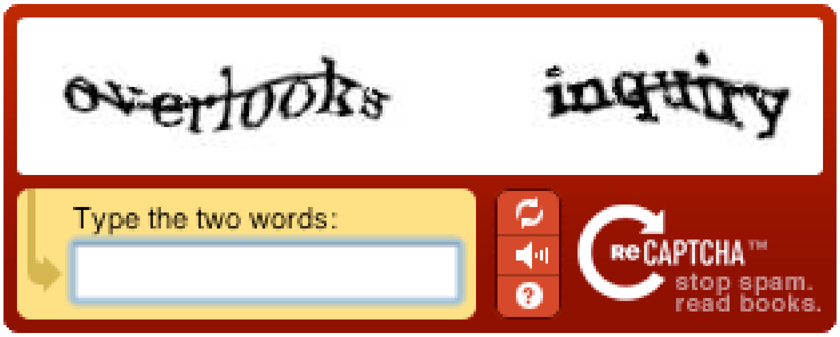
> The key is a simple file called *robots.txt* that has been an industry standard for many years. It lets a site owner control how search engines access their web site. With *robots.txt* you can control access at multiple levels -- the entire site, through

[24] http://www.dmnews.com/list/1280.html.
[25] http://www.dmnews.com/list/623.html.
[26] Charles Duhigg, *Bilking The Elderly, With Corporate Assist*, THE NEW YORK TIMES, May 20, 2007, *available at* http://www.nytimes.com/2007/05/20/business/20tele.html
[27] *Id.*

> individual directories, pages of a specific type, down to individual pages.[28]

We recommend an adequately configured *robots.txt* file that prevents major search engines from indexing any online court records.

The *robots.txt* system is voluntary -- major search engines respect it, but it does not serve as a technical bar. Another technical device used to prevent automatic remote access is a CAPTCHA -- "a program that can generate and grade tests that humans can pass but current computer programs cannot."[29] The site presents an example:[30]



A human user can read the two words, a computer program cannot. Visually impaired users can use the middle button to hear the words. CAPTCHA's are specifically recommended to keep information from being searched:

> It is sometimes desirable to keep webpages unindexed to prevent others from finding them easily. There is an html tag to prevent search engine bots from reading web pages. The tag, however, doesn't guarantee that bots won't read a web page; it only serves to say "no bots, please." Search engine bots, since they usually belong to large companies, respect web pages that don't want to allow them in. However, in order to truly guarantee that bots won't enter a web site, CAPTCHAs are needed.[31]

The reCAPTCHA service here used as an example is available for free.[32]

Another solution to the data broker problem is to prohibit remote access for those who intend the resale of records gained via remote access.[33] California placed a

[28] *Controlling How Search Engines Access and Index Your Website*, The Official Google Blog, Jan. 26, 2007, http://googleblog.blogspot.com/2007/01/controlling-how-search-engines-access.html.

[29] What is a CAPTCHA?, http://recaptcha.net/captcha.html.

[30] *Id.*

[31] *Id.*

[32] Get reCAPTCHA, http://recaptcha.net/whyrecaptcha.html.

[33] *See* use limitations listed *supra*, notes 19 and 20.

restriction on the release of arrestee addresses.[34] Generally, releases could only be made "where the requester declares under penalty of perjury that the request is made for a scholarly, journalistic, political, or governmental purpose, or that the request is made for investigation purposes by a licensed private investigator."[35] Further, the addresses could not be sold, nor used to sell a product.[36] The Supreme Court rejected a facial challenge to this law.[37]

Legal restrictions on access to electronically aggregated public records are a legitimate method of privacy protection. As EPIC stated in its comments to the Florida courts:

> [T]he [Supreme] Court has recognized legitimate privacy interests that qualify a right to access public records and other records held by government. In *DOJ v. Reporters Committee for Freedom of the Press*, the Court denied access to criminal "rap" sheets, aggregate summaries of criminal histories compiled from multiple jurisdictions. [489 U.S. 749 (1989)]. The Court in that case found a privacy interest in information that was publicly accessible, but because it was stored in courthouses across the country, the information remained "practically obscure." [*Id.*] In denying access to the rap sheets, the Court noted that, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." [*Id.* at 764].[38]

VI. PROPOSED POLICY

It is the position of the undersigned that the Court should not move information online until it has the resources to properly implement this policy. We also note that the Family Violence department of the National Council of Juvenile and Family Court Judges is developing recommendations for placing court records online.[39] These recommendations will be available by mid 2008.[40] We further recommend that the court not place records online until these recommendations are available.

The proposed policy aims to follow the appropriate laws, respect established

[34] Los Angeles Police Department v. United Publishing Group, 528 U.S. 32 (1999).

[35] *Id.* at 35.

[36] *Id.*

[37] *Id.* at 37.

[38] Electronic Privacy Information Center, *Comments to the Committee on Privacy and Court Records* 8 (Nov. 1, 2004), *available at* http://www.epic.org/privacy/publicrecords/flcomments.pdf

[39] Email from Roberta Valente, Assistant Director, Family Violence Department NCJFCJ, to Guilherme Roschke, Skadden Fellow, EPIC (Oct. 9, 2007) (on file with Guilherme Roschke).

[40] *Id.*

minimum standards for privacy, and promote convenient access to court records.

1. The court should follow the VAWA mandates:

   a. No CPO Docket information should be publicly published online.
   b. No notations of a CPO should be publicly published online in other Dockets
   c. No civil restraining order should be publicly published online.
   d. No Domestic Relations docket information should be publicly published online.
   e. No complaining witness, stay away, or CPO notations should be publicly published online in the criminal dockets

.

2. Additional safeguards based on Fair Information Practices should be established:

   a. Openness: The Court should clearly inform litigants of its records publishing policies at the time of filing or of service of process.
   b. Security Safeguards: Technical standards similar to the ones listed above should be implemented to prevent bulk downloading and unauthorized access. Use of online court records should be limited to a password based login system for authorized purposes.
   c. Use Limitation: A set of legitimate purposes, including litigant convenience, should be established in granting online record access. These limitations should explicitly exclude commercial re-sale or bulk downloading of information. Online publication should be done only with the consent of the individual whose information is published.
   d. Data Quality: Records published online should be published only in correct form, and not include any errors.
   e. Accountability: Individuals should have access to a Committee or other review procedure in order to ensure that their privacy is protected. This procedure should enforce VAWA mandates as well as the established privacy policy.

We welcome this opportunity to comment and look forward to continuing to provide input on this issue as online access policies are developed.

Respectfully Submitted,

Marc Rotenberg	Guilherme Roschke
Executive Director	Skadden Fellow
Electronic Privacy Information Center	Electronic Privacy Information Center

Lisa Vollendorf Martin
Clinic Associate,
Families and the Law Clinic
Columbus School of Law,
Catholic University of America[*]

Professor Deborah Epstein,
Georgetown University Law Center[*]

Legal Aid Society of The District Of Columbia

Yvette Garcia Missri
Assistant Attorney General,
Domestic Violence section
Office of the Attorney General for DC[*]

Professor Laurie Kohn,
Georgetown University Law Center[*]

Ayuda, Inc.

Break the Cycle

[*] Affiliation provided for identification purposes only.