2005

Internet Access to Court Records: Balancing Public Access and Privacy

Natalie Gomez-Velez

CUNY School of Law

How does access to this work benefit you? Let us know!

Follow this and additional works at: http://academicworks.cuny.edu/cl_pubs

Part of the Law Commons

Recommended Citation

http://academicworks.cuny.edu/cl_pubs/209

This Article is brought to you for free and open access by the CUNY School of Law at CUNY Academic Works. It has been accepted for inclusion in Publications and Research by an authorized administrator of CUNY Academic Works. For more information, please contact AcademicWorks@cuny.edu.
ARTICLES

INTERNET ACCESS TO COURT RECORDS - BALANCING PUBLIC ACCESS AND PRIVACY

Natalie Gomez-Velez*

TABLE OF CONTENTS

INTRODUCTION ................................................................. 367
I. BACKGROUND: GENERAL INTERNET PRIVACY CONCERNS AND THE LAW'S RESPONSE .......... 373
   A. THE BROADER PROBLEM: ONLINE AGGREGATION AND DISSEMINATION OF PERSONAL INFORMATION ..... 374
   B. INDUSTRY SELF-REGULATION VERSUS THE CALL FOR GREATER GOVERNMENT REGULATION TO PROTECT INTERNET PRIVACY .......................................................... 377
   C. PRIVACY LAW AND ITS APPLICATION TO THE

* Assistant Professor of Law, City University of New York School of Law. The author served as Special Counsel to the Chief Administrative Judge of the State of New York and was staff counsel to New York State's Commission on Public Access to Court Records. However, the opinions expressed in this article do not necessarily reflect the views of the New York State Courts or the Commission. The author gratefully acknowledges Chief Judge Judith S. Kaye and Chief Administrative Judge Jonathan Lippman for introducing her to this topic and supporting her work. The author also thanks her former colleagues, Mary C. Mone, Antonio Galvao, Amy Vance, Martha Wade Steketee, David M. Nocenti, and Ken Dreifach for helpful discussions about Internet privacy and court records access. The author thanks her colleagues, Ruthann Robson, Andrea McArdle, Rebecca Bratspies, Julie Lim, members of the scholarship group, and her husband, Roberto Velez for their helpful comments and invaluable support in completing this article, as well as the Professional Development Committee of CUNY School of Law, for providing funds for research assistance to support the work of John Rodrigues, Yasemin Ekici, and Elain Berger.

365
II. THE INTERNET PROMISES GREATER PUBLIC ACCESS TO COURT RECORDS AND GREATER TRANSPARENCY OF COURT FUNCTIONS, BUT HIGHLIGHTS THE PERCEIVED DIFFICULTY IN PROTECTING INDIVIDUAL PRIVACY WHILE PREVENTING GOVERNMENT SECRECY

A. PUBLIC ACCESS TO GOVERNMENT RECORDS IS GENERALLY VIEWED AS AN ANTIDOTE TO GOVERNMENT SECRECY

B. THE LAW RECOGNIZES A CONSTITUTIONALLY-BASED, THOUGH QUALIFIED, RIGHT OF PUBLIC ACCESS TO COURT RECORDS

C. CONCERNS ABOUT SECRECY COMPLICATE COURT EFFORTS TO BALANCE PUBLIC ACCESS AND PRIVACY WHEN PLACING COURT RECORDS ON THE INTERNET.

III. THE COMBINATION OF PRIVATE AND PUBLIC SECTOR INFORMATION GATHERING AGGREGATION, AND DISSEMINATION IMPACT PUBLIC ACCESS/PRIVACY CONCERNS IN THE COURT RECORDS CONTEXT

IV. RECOMMENDATIONS FOR DEVELOPING POLICIES THAT BALANCE THE TENSION BETWEEN PUBLIC ACCESS AND PRIVACY IN THE COURT RECORDS CONTEXT

A. COURTS MUST CONFRONT THE POLICY CHALLENGE RAISED BY THE PROSPECT OF INTERNET ACCESS TO COURT RECORDS WITH A COHERENT POLICY THAT DRAWS UPON EXISTING FRAMEWORKS AND THE EXPERIENCES OF OTHER COURTS IN STRIKING THE PUBLIC ACCESS/PRIVACY BALANCE

B. IT IS IMPERATIVE THAT COURTS INCLUDE STAKEHOLDERS IN THE POLICY DEVELOPMENT PROCESS
C. Court Records Access Policies Must Respect the Unique Role of the Courts in Our System of Separated Powers and Checks and Balances 426

D. Court Records Access Policies Should Begin with Existing Court Record Closure Rules and Consider Whether Those Rules Suffice or Should Be Adapted or Amended in Light of Internet Access ........................................................ 427

E. Court Records Access Policies Should Identify and Remove from Public View High Risk Data Elements That Do Not Serve the Purposes of Public Access .................................................. 429

F. Courts Should Affirmatively and Aggressively Educate the Bench, the Bar and the Public About the Implications of Internet Access to Court Records ........................................ 435

CONCLUSION .................................................................................. 436

INTRODUCTION

Federal and state courts across the country are becoming publicly accessible as never before. Growing reliance on computer technology generally and on the Internet specifically, has made the prospect of placing court case records and information online via the Internet a reality. Yet, as courts around the country are discovering, difficult policy questions arise as courts move from paper to electronic records, move beyond providing online access to court calendars and docket information, and begin making case files themselves available over the Internet.

1. One court has described the internet as follows:
   The Internet is accurately described as a 'network of networks.' Computer networks are interconnected individual computers that share information. Anytime two or more computer networks connect, they form an 'internet.' The 'Internet' is a shorthand name for the vast collection of interconnected computer networks that evolved from the Advanced Research Projects Agency Network ("ARPANet") developed by the United States Defense Department in the 1960's and 1970's. Today, the Internet spans the globe and connects hundreds of thousands of independent networks. The World Wide Web ("the Web" or "WWW") is often mistakenly referred to as the Internet. However the two are quite different. The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables and routers through which data is shared online. The Web is data: a vast collection of documents containing text, visual images, audio clips and other information media that is accessed through the Internet.

Over the past several years, federal and state courts across the country have been making court-related information available electronically over the Internet. A number of state courts have provided Internet access to court calendars, indices, rules, and decisions for a few years now. More recently, the federal courts and a handful of state courts have begun the process of making case records—the actual documents filed in a case—available for the first time over the Internet.


Internet access to court records promises greater public access and greater transparency of court functions. It raises concerns, however, about the broad dissemination of individual private or sensitive information contained in court records. The strongest arguments in favor of making court records available online are that Internet access increases public access and serves the interest in “sunshine” or public oversight of the court system. The ability to access court records online will make it easier to obtain those records to review the workings of the courts both as a general matter and in particular cases and classes of cases. This availability, its proponents hope, will help demystify court procedures and will support greater public education, accountability, and public confidence. Providing online access to court records may also serve broader efficiency interests in the areas of records access, records management, case management, and electronic filing.


5. See, e.g., HON. JONATHAN LIPPMAN, REPORT ON THE NEW YORK STATE UNIFIED COURT SYSTEM FILING BY ELECTRONIC MEANS AND FILING BY FACSIMILE TRANSMISSION PILOT PROGRAMS PURSUANT TO CHAPTER 367 OF THE LAWS OF 1999 at 22, http://www.courts.state.ny.us/reports/FBEM.pdf. Lipmann states:

As all three branches of New York State government contemplate the future, it is clear that more and more business between State residents and their government will be done on an electronic basis . . . computer-based interactive transactions provide individuals with rapid, cost-effective access to government
Strong opposition exists, however, to placing court records online. Some opponents argue that the benefits for purposes of public access and "sunshine" will be minimal. Further, opponents warn that the newly available court record information will be used for private and largely nefarious purposes, such as data mining, stalking, and snooping, which have nothing to do with public education or court accountability.6 To these opponents, the risks associated with making court records available online (as opposed to allowing access only to docket information and court decisions) outweigh the benefits of greater public access and transparency. This is because court records, although public, often contain sensitive personal information. Although this information has always been in court records, opponents argue that paper records are "practically obscure"7 in comparison to online records. Obtaining paper records requires a trip to the courthouse with a party name or index number to retrieve a particular case record, or hours of reviewing multiple files to support a broader inquiry. Because court records were deemed "practically obscure," there was little concern about the

services from virtually anywhere.


7. In United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989), the Supreme Court commented on the phenomenon of practical obscurity: "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."
dissemination of personal information from such records.

Providing Internet access to court records increases exponentially the availability of court records, including any sensitive information they contain. Examples of sensitive information that might be found in court records include: social security numbers, home addresses, names of minor children, financial account numbers, and medical information. Online court records raise concerns that these and other kinds of sensitive information will be used for improper purposes such as identity theft, stalking, discrimination, locating domestic violence victims, and interference with business and social relationships, rather than for the appropriate oversight, educative, and accountability reasons for which court records are made public.

8. As noted in a report by the Electronic Privacy Information Center:
Court records contain a wealth of personal information. For instance, bankruptcy filings, which are required by statute to be public, contain personal identifiers and detailed information on the petitioners' assets. Civil case files may contain medical information and detailed information on spousal infidelity and abuse. Criminal case files may contain presentencing reports and the identity of officers and witnesses in criminal investigations.


Electronic searching and compiling technologies can convert electronic court records into a veritable treasure trove of personal information about a vast range of individuals. Searching across both years and different jurisdictions, one can easily accumulate a dossier or compile a profile of an individual—valuable in a number of undesirable manners, ranging from marketing to extortion and identity theft.


Many state courts involved in developing policies governing Internet access to court records heard testimony about various ways in which the information in court records might be used improperly. For example, New York's Commission on Public Access to Court Records heard concerns about identity theft:

Identity thieves often combine "high value" personal identification, such as bank account or social security numbers, with "low value" information more readily available to the public, such as name, address, or birth date. Along this spectrum lies other data, readily available about some people, but not others: for instance, a prominent attorney's mother's maiden name, might be listed in Who's Who in America, along with his place and date of birth and his children's names (which may make his password easy to guess, as well); a CEO's signature might be accessible for forgery from her company's annual report (as attorneys signatures are available in scanned PDF documents online). Court records often contain the type of information most often used in identity theft, especially in consumer cases or class actions.

Ken Dreifach, Chief, Internet Bureau, Office of New York Attorney General to New York State Commission on Public Access to Court Records 2-3 (May 30, 2003),
This article addresses the current debate between public access and privacy in courts around the country as many courts begin providing Internet access to court docket information and case records. Section I provides background about the general concerns about Internet privacy that inform the debate about placing court records information online, and sketches the sources and limitations of legal privacy protection, specifically protection of “information privacy.” Section II addresses the competing interest in public access and government transparency in the court records context. This section also addresses the difficulty courts face in protecting individual privacy while avoiding charges of government secrecy. Section III explores the effect of the combination of private and public sector data compilation on the debate. Finally, Section IV proposes that courts must confront the policy challenge presented by Internet access. In developing court records access policies, courts should include stakeholders, while respecting the courts’ role in our tripartite system of government and the purposes of public access. The effective protection of both individual privacy/security and government transparency begins with a re-

http://www.nycourts.gov/ip/publicaccess/Exhibit3.pdf. The Commission also heard concerns about domestic violence and stalking victims:

[A]busers often track and monitor their victims as a means of maintaining control. These behaviors typically increase when a victim leaves the abuser. Whenever a victim becomes involved with the court system, whether voluntarily, as a result of mandatory arrest or pro-prosecution policies or for some other reason, precious information about her location, status, current name, phone numbers and other circumstances is disclosed. Such disclosure is a major concern... We know that abusers will access this information and use it every way possible to stalk, threaten, assault, or kill the victim and maybe her children. This can be a problem even where the victim is using the court system for something other than domestic violence. For example, if she is involved in a motor vehicle accident resulting in legal action and the information, including the location of the court, is posted on the Internet, her address would be posted making it all too easy for her abuser to find her.

Charlotte A. Watson, Executive Director, New York State Office for the Prevention of Domestic Violence before the Commission on Public Access to Court Records 3-4 (May 30, 2003), http://www.nycourts.gov/ip/publicaccess/Exhibit3.pdf. On the other hand, some commentators noted possible positive consequences for victims in placing court records online:

But the Internet cuts both ways. McDonald eventually used online court, property and death records to show her ex-husband was lying about his finances, she says. When her ex-husband began coming to child custody hearings in brand new cars, she found and undisclosed $261,000 from the sale of his late father’s vacation home. As a result, a judge increased his child support payments. Now he owes more than $20,000 in child support—and she can’t find him.

assertion of the balances already struck with respect to government records generally and court records in particular. However, because the Internet is causing the courts to respond to concerns that go well beyond court records, adequate protection also calls for courts to consider excising from court records high risk information that is of low value from a public accountability perspective and to affirmatively educate the bench, the bar, and the public about the implications of Internet access.

I. BACKGROUND: GENERAL INTERNET PRIVACY CONCERNS AND THE LAW'S RESPONSE.

He thought of the telescreen with its never-sleeping ear. They could spy upon you night and day, but if you kept your head you could still outwit them . . . . They could lay bare in the utmost detail everything that you had done or said or thought; but the inner heart, whose workings were mysterious even to yourself, remained impregnable.

George Orwell, 1984, Part 2, Chapter 7 (Plume, 2003, c1979)

The Internet and its supporting architectures have made it much easier to track and monitor individual behavior. Identifying serial numbers embedded within computer chips or software programs that allow traces to an end user's identity threaten to end the electronic anonymity that has so far characterized many interactions in cyberspace. And Web bugs and cookies\(^\text{10}\) allow for an unprecedented level of surreptitious Internet surveillance.

Richard A. Spinello, CyberEthics, Morality and Law in Cyberspace 141 (2002)

For many people concerned about individual privacy, the Internet exemplifies the realization of the Orwellian nightmare of a society devoid of privacy in which an unseen "Big Brother" observes, collects, and compiles everything there is to know about individuals and uses that information to control activities, behaviors, and even thoughts. Concerns about the privacy and security of personal information contained in court records are

\(^{10}\) "Cookies" is a computer science term defined as "a collection of information, usually including a username and the current date and time, stored on the local computer of a person using the World Wide Web, used chiefly by web sites to identify users who have previously registered or visited the site." Dictionary.com, http://www.dictionary.reference.com/search?q=cookies%20.
directly related to broader concerns about commercial and
government uses of personal information gathered online,
aggregated (often together with offline information), and used for
purposes unknown to (and in some instances not even imagined
by) the data subjects. This lack of knowledge on the part of
individuals about what personal information is being collected,
together with the vast, unprecedented types and quantities of
information that may be amassed using Internet technology has
raised red flags with respect to all data provided online.

A. THE BROADER PROBLEM: ONLINE AGGREGATION AND
DISSEMINATION OF PERSONAL INFORMATION

Recent reports about far-reaching breaches of security in the
computer databases of several companies, from Lexis/Nexis, to
ChoicePoint, to DSW Shoes (a shoe store franchise) have
heightened public concern about identity theft and other misuses
of personal information stored in computer databases that are
shared and aggregated online. This concern dates back several
years and the commercial and governmental responses have
contributed to the current dilemma facing courts and other
government policymakers when confronted with the need to
balance individual privacy and security concerns with the
interests in providing convenient, broad access to public records,

11. The fact that individuals are largely unaware of the collection and use of their
private information is described by some commentators as the “problem” of privacy in
cyberspace.

Real-space architecture makes surveillance generally self-authenticating.
Ordinarily we can notice if we are being followed, or if data from an identity card
is being collected. Knowing this enables us to decline giving information if we do
not want the information known. Thus, real space interferes with the non-
consensual collection of data. Hiding that one is spying is relatively hard. The
architecture of cyberspace does not similarly flush out the spy. We wander
through cyberspace, unaware of the technologies that gather and track our
behavior .... To consent to being tracked, we must know that data is being
collected. But the architecture disables (relative to real space) our ability to
know when we are being monitored, and to take steps to limit the monitoring.

Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 113 HARV. L.

12. See Privacy Rights Clearinghouse, A Chronology of Data Breaches Since the
ChoicePoint Incident, (April 20, 2005), http://www.privacyrights.org/ar/ChronDataBre
aches.htm; see also Tom Zeller, Jr., Another Data Broker Reports a Breach, New
York Times, March 10, 2005 at C1 (reporting LexisNexis database breach); Paul
Roberts, Hackers Breach LexisNexis, Snatch Consumer Data, COMPUTERWORLD,
00317,00.html; Emily Hackett, The Problem of Data Security, TRUSTe Policy Flash,
0050421012042&list=policyflash.
to improve transparency and foster more efficient administration.

News about the acquisition and aggregation of large amounts of personally identifiable information including name, age, address, work information, financial information, property ownership, purchasing habits, medical information, and even clickstream\(^3\) data, by unknown commercial entities caused great concern among privacy advocates and the public. This concern turned to outrage on the eve of the millennium, when certain data profiling practices became public.

For example, when online advertiser DoubleClick's plans to combine online clickstream data with data collected offline that would identify individual users and information about them (including user's name, address, retail, catalog, and online purchase history, and demographic data) came to light, the public outcry led to an investigation by the Federal Trade Commission, a lawsuit by the State of Michigan, and a consumer class action alleging that DoubleClick's collection and use of Internet data was improper.\(^14\) The plaintiffs' complaint was dismissed because the alleged violations did not meet the requirements for finding liability under the Electronic Communications Privacy Act, the Federal Wiretap Act, or the Computer Fraud and Abuse Act.\(^15\) Nevertheless, partly in response to the negative publicity when DoubleClick's practices were revealed, DoubleClick agreed to a settlement.\(^16\) The settlement provided, among other things, that if personally identifiable information is collected, that information can only be combined with clickstream data after DoubleClick provides clear and conspicuous notice to the Internet user and obtains the Internet user's opt-in choice.\(^17\) The settlement also provided that "the company's privacy policy will include easy-to-read

\(^{13}\) "Clickstream" is defined as "a series of mouse clicks made by a user of the Internet, especially logged and analyzed for marketing research; the virtual record of an Internet user's activity including every Web site and every Web page visited and how long the user was at each." Dictionary.com, http://dictionary.reference.com/search?q=clickstream.


\(^{15}\) Id. at 526.

\(^{16}\) In re DoubleClick, Inc. Privacy Litigation, Master File No. 00-CIV-0641 (NRB), 2002 U.S. Dist. LEXIS 27099.

\(^{17}\) See Court Approves DoubleClick Settlement; Net Advertiser to Institute New Protections, UNITED STATES LAW WEEK, May 28, 2002, available at Westlaw, 70 USLW 2742.
explanations of its online ad services . . . and [DoubleClick] will undertake a consumer education effort, which includes 300 million consumer privacy banner ads that invite consumers to learn more about how to protect their online privacy." Several other class action lawsuits have been commenced by private parties against various companies engaging in commercial aggregation of personal information utilizing the Internet. As in the DoubleClick case, litigants claimed that "various online activities have violated the privacy rights of individual users of the Internet."20

Concerns about Internet privacy are not limited to a few zealous plaintiffs. Studies have long demonstrated significant public concern about surreptitious online monitoring. For example, an FTC report issued in 2000 found "[ninety-two percent of those surveyed say that they are concerned about threats to their personal privacy when they use the Internet and seventy-two percent say they are very concerned."21 Furthermore, ninety-five percent expressed grave concern about the aggregation of their personal information, specifically, "income, driver's license, credit data, and medical status . . . ." Internet users also are wary of companies selling their personal information to third parties. "Ninety-two percent say that they are not comfortable with Web sites sharing their personal information . . . and 93% are uncomfortable with their information being sold."22 One survey mentioned in the FTC Online Profiling report states that consumers are willing to


19. See, e.g., In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 16 (1st Cir. 2003) (alleging that certain Defendants had intercepted electronic communications without Plaintiff's consent in violation of the Electronic Communications Privacy Act of 1986); In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) (discussing suit computer users brought against website operator, alleging violation of privacy rights through implementation of "cookies").


23. Id. at 16.
provide certain personal information if they are given notice and choice. However, "the statistics also demonstrate that many consumers are not willing to allow this kind of profiling regardless of whether choice and notice are given." 

In the wake of revelations about the aggregation and dissemination of individual information via the Internet, coupled with evidence of public concern about Internet privacy, many called upon government regulators to provide greater protection of "information privacy." Some even argued that the degree to which detailed personal profiles of individuals can be developed by combining and networking various databases of information without the subjects' knowledge or consent and without their ability to correct errors or learn of the uses to which their information is being put, raises significant concerns about the very meaning and salience of "information privacy" in the Internet age.

B. INDUSTRY SELF-REGULATION VERSUS THE CALL FOR GREATER GOVERNMENT REGULATION TO PROTECT INTERNET PRIVACY

In response to the increasing public concerns about the aggregation, combination, and dissemination of vast amounts of personal information, many Internet businesses and free-market advocates argued that individual consumer privacy could best be protected through industry self-regulation. Positing that

---


26. See, e.g., Marcia S. Smith, Internet Privacy: Overview and Pending Legislation, Report for Congress, CRS-3, (Feb. 6, 2003), http://www.epic.org/privacy/internet/RL31408.pdf ("Consumer, privacy rights and other interest groups believe self-regulation is insufficient. They argue that the seal programs do not carry the weight of law, and that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy.").


government regulation of the Internet would stifle this fledgling technology, they argued that effective self-regulation would offer greater protection to individuals because Internet businesses and service providers had an incentive to self-regulate and protect consumer privacy as a matter of customer service and industry competition. Companies that wanted to stay in business would ensure that their customers felt secure in their Internet transactions.  

The incentives to gather and share information for purposes of target marketing, however, have thus far proven much stronger than the incentive to protect consumer privacy through industry self-regulation. As several commentators observe, the market in detailed, aggregated personal information obtained over the Internet is a lucrative business, which offers very little incentive to protect individual privacy. "The field is a large one that is rapidly growing larger, because consumer information is an extremely valuable asset . . . . The revenues of the biggest data-mining companies exceed $1 billion annually . . . some companies reportedly earn more from selling customer lists than from selling their own goods or services."  

privacy sends a distinctly different message from what they say.

29. Another argument supporting the free use of individual personal information for target marketing highlights the benefits of such use (for customers as well as businesses) as outweighing any costs to individuals: "After all, the use of personal information about consumers results in significant benefits for everyone. For example, businesses that know a lot about their customers can obviously improve their efficiencies in marketing, distribution and product development. This knowledge inarguably leads to the delivery of less expensive and more useful products and services. Customers are therefore, largely trading privacy for a more efficient marketplace. Perhaps because of these benefits, the loss of some personal privacy is appears quite benign." Craig D. Tindall, Argus Rules: The Commercialization of Personal Information, 2003 U. ILL. J. L. TECH. & POLY 181, 183 (2003).

30. See, e.g., Oscar H. Gandy, Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace, 1996 U. CHI. LEGAL F. 77, 79 ("the pressures will only increase on product and branch managers to learn ever more about consumers, including the most efficient and effective way to capture their attention and secure their agreement to buy"); Joel R. Reidenberg & Francoise Gamet-Pol, The Fundamental Role of Privacy and Confidence in the Network, 30 WAKE FOREST L. REV. 105, 119 (1995) (noting the United States' rejection of "proposals for a fair information practices code due to the strong opposition of American business lobbies").

In addition, companies have a financial incentive to obtain users’ personal information because studies show that direct marketing receives a more favorable response than random ads sent to online users. Finally, fierce competition on the Internet results in increased reliance by Web site operators on direct marketers to attract and retain customers.\(^{32}\)

The extraordinarily lucrative market for compiled and aggregated personal information has fostered robust resistance to government regulation to protect individual privacy. The Federal Trade Commission ("FTC") initially was persuaded by industry warnings that government regulation would stifle the development of the Internet economy. The FTC thus supported industry self-regulation. "These efforts have been based on the belief that greater protection of personal privacy on the Internet will benefit businesses as well as consumers by increasing customer confidence in the online marketplace."\(^{33}\) The FTC urged companies to self-regulate, recommending that:

Consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices: (1) notice—web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site, (2) choice—web sites would be


[Surveillance of users on the Internet is cheap, and its product (profiles) is extremely valuable. The result is a simple economic incentive to engage in surveillance of everyone online, everywhere, all the time, and to compile and maintain finely granulated records on the entire population of the Internet. Never before in the history of civilization has such surveillance been possible... because cyberspace has radically decreased the cost of collecting data, what might have been economically justified only for the targets of extraordinary investigations is now justified for the average Jane.

Jenab, supra note 31.


required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided . . . (3) access—Web sites would be required to offer consumers reasonable access to the information a Web site has collected on them, including reasonable opportunity to review the information and to correct inaccuracies or delete information, (4) security—Web sites would be required to take reasonable steps to protect the security of the information they collect.\(^{34}\)

The Network Advertising Initiative, a group of network advertisers, was established in 1999 to develop a set of privacy principles.\(^{35}\) The NAI worked in conjunction with the FTC on developing guidelines for Internet industry self-regulation, but, as noted in an FTC report, despite its significant work in developing self-regulatory initiatives, “industry efforts alone have been insufficient.” Thus, the majority recommended that Congress enact legislation to ensure consumer privacy online.\(^{36}\)

While strong market forces favoring increased consumer information gathering and compilation have served to limit effective industry self-regulation to protect individual consumer privacy interests, government has found itself caught between the pressures of free market business interests in avoiding government regulation of the Internet and the clear concerns of members of the public and privacy advocates about individual privacy and security in Internet transactions.

Privacy advocates viewed the lack of strong government regulation to protect Internet users as a betrayal of government’s mandate to protect individual privacy as a “fundamental” interest. Of course, fundamental, constitutionally-based privacy protection applies only as against government intrusion. As noted below, the protection of “information privacy” as against private actors is based on a patchwork of common law, statutory and regulatory provisions which are often insufficient to address the intrusions on individual privacy and security made possible by Internet technology.

While the FTC, Congress, and other government regulators

\(^{34}\) FTC REPORT, supra note 33, at iii.

\(^{35}\) See Network Advertising Initiative Website, http://www.networkadvertising.org/about/privacy.asp (defining the NAI online privacy principles).

\(^{36}\) See FTC REPORT, supra note 33 at ii-iii, 35-36.
now see the need for government regulation of Internet privacy and security, they have a way to go before finding effective regulatory solutions. Part of this difficulty has to do with the legal framework supporting privacy protection in the Internet context, which in turn stems from the nature of existing privacy protection as against both governmental and private intruders. Another part of the difficulty stems from the nature of, and pressures on, the legislative process.

C. PRIVACY LAW AND ITS APPLICATION TO THE INTERNET

The right to privacy, though not explicitly stated in the Constitution, is based on constitutional principles and is implicit in the Bill of Rights, and in concepts of liberty and due process. As the Supreme Court articulated in Griswold v. Connecticut, "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance... Various guarantees create zones of privacy." Thus, Justice Douglas found a right to privacy to be implicit in several Constitutional amendments: the First, Third, Fourth, Fifth, and Ninth. In striking down a Connecticut statute that prohibited doctors from advising married couples in the use of contraceptives, Justice Harlan said that the statute "infringe[d] the Due Process Clause of the Fourteenth Amendment [and] violate[d] basic values implicit in the concept of ordered liberty."

37. I provide here only a brief overview of privacy law and its application to the Internet. For extensive discussions of Internet privacy law, see, for example, Daniel J. Solove, Access and Aggregation, supra note 27; Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193 (1998); Susan E. Gindin, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 SAN DIEGO L. REV. 1153 (1997); Ken Gormley, One Hundred Years of Privacy, 1992 Wis. L. REV. 1335 (1996); Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. ILL. U. L. REV. 479, 506-08 (1990).


39. Justice Douglas explained:

The right of association contained in the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution of certain rights, shall not be construed to deny or disparage others retained by the people.'

Id. at 484.

40. Griswold, 381 U.S. at 500.
The Supreme Court has used similar terms to articulate a fundamental right of privacy in a number of different contexts.\(^{41}\)

Perhaps the most straightforward constitutional statement of privacy protection is contained in the Fourth Amendment.\(^{42}\) Fourth Amendment privacy protection applies against government intrusion and is based on "reasonable expectations of privacy." This can be shaky foundation in the Internet age.\(^{43}\) As the Supreme Court noted in *Katz v. United States*,\(^{44}\) a case involving electronic eavesdropping in a public telephone booth, "[t]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."\(^{45}\) In the age of Internet technology as well as increasingly sophisticated and intrusive surveillance technology (like hidden cameras and even cell phone cameras) some commentators have labeled the Fourth

---

41. See, e.g., Loving v. Virginia, 388 U.S. 1, 12 (1967) (discussing privacy right relating to inter-racial marriage); Roe v. Wade, 410 U.S. 113, 165 (1973) (examining decisional privacy right to an abortion); Zablocki v. Redhail, 434 U.S. 374, 383 (1978) (holding that right to marry is part of the "right of privacy" implicit in the Fourteenth Amendment); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (finding the right to contraception even for unmarried persons part of right of privacy); Planned Parenthood v. Casey, 505 U.S. 833, 839 (1992) (reaffirming essential holding from Roe v. Wade recognizing woman's right to choose abortion as part of decisional privacy right).

42. The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but on probable cause supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

U.S. CONST. amend. IV. As one commentator notes:

If privacy was explicitly acknowledged anywhere in the early contours of American law, it was within the folds of criminal procedure, where even in the early days of colonial life there existed a strong principle, inherited from English law, that a 'man's house is his castle; and while he is quiet, he is well guarded as a prince in his castle.'

Gormley, *supra* note 37, at 1358.

43. The erosion of Fourth Amendment privacy protection also has been noted with respect to the government's war on drugs and other "subject matter" such as recent concerns about terrorism following the attacks of September 11, 2001. See Gormley, *supra* note 37, at 1370; see also, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 CAL. L. REV. 1083, 1133 (2002); Marc Rotenberg, *Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1117-19 (2002).


45. *Id.*
Amendment's protection of privacy based on a "reasonable expectation" of privacy not only circular, but at risk of offering very little protection at all.46 As one commentator has put it:

Although the consequences are paradoxical, evolving legal standards suggest that as an individual's expectation that he is under surveillance increases, the scope of his expectation of privacy decreases. Under a governing interpretation of the Fourth Amendment (and common law extensions to private entities), individuals who engage in activities that they know, or should know, may be subject to surveillance are often treated as having granted consent for such surveillance.47

Adding to the confusion fostered by the changeable and perhaps eroding Fourth Amendment privacy right, there is a general lack of clarity or consensus about how to define and protect privacy under law.

First, there is no consensus on the interests that comprise privacy. For instance, Jerry Kang describes three "clusters" privacy concerns with regard to (1) physical space ("spatial privacy"), (2) choice, and (3) the flow of personal information. However, Anita Allen-Castellitto divides privacy in "at least four basic types": (1) informational privacy, (2) physical privacy, (3) decisional privacy, and (4) proprietary privacy. Meanwhile, the fathers of privacy law, Samuel Warren and Justice Louis Brandeis, described a "general right of privacy for thoughts, emotions, and sensations [that] should receive the same protection, whether expressed in writing or in conduct, in conversation, in attitudes, or in facial expression."

These privacy paradigms help identify the ways in which courts have analyzed privacy interests. However, as with other attempts to pin down both the parameters of the privacy right and the nature of privacy interests, the effort to define and locate


the sources and limits of information privacy remains very
difficult, particularly in the context of the Internet intrusions,
which may be deemed both voluntary and involuntary and which
may be described as falling within or outside of the various
traditional privacy constructs. Some of this is due to the nature
of the privacy concept and its need to conform to changing
circumstances. As Ken Gormley puts it: “[t]he tiger has chased
its tail with respect to the ongoing quest for a single definition of
privacy only because privacy (inherently) is not a static concept,
any more than democracy or American life are static conditions.”

In addition, even as courts, legal scholars and judges
struggle to define privacy's parameters, there are concerns that
constitutionally based privacy protections are eroding. For
example, while the Court in Katz held that Fourth Amendment
privacy protection is not limited to physical intrusions (as it had
been under the Supreme Court's earlier decision in Olmstead v.
United States), but is based on "reasonable expectations of
privacy." This test establishes a conception of Fourth Amendment
privacy that tends to protect only matters that
private individuals have kept "secret," thus severely limiting its
applicability to the kinds of privacy concerns raised in the
technological age. As Daniel Solove observes:

The "reasonable expectation of privacy test" looks to whether
(1) a person exhibits an "actual or subjective expectation of
privacy" and (2) the expectation [is] one that society is
prepared to recognize as reasonable . . . . Although we have
moved from the . . . Olmstead world of physical papers and
places to a new regime based upon expectations of privacy,
there is a new Olmstead, one that is just as shortsighted and
rigid in its approach. The Court's new conception of privacy
is one of total secrecy. If any information is exposed to the
public or if law enforcement officials can view something
from any public vantage point, then the Court has refused to
recognize a reasonable expectation of privacy. 50

The Supreme Court's application of the "reasonable
expectation of privacy" test has developed somewhat unevenly at
best and at worst appears to have fostered a continuing erosion of
the right of privacy. For example, the Court has found

49. Gormley, supra note 37, at 1342.
50. Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment
“reasonable” expectations of privacy in homes, businesses, sealed luggage and packages, and even drums of chemicals, but no “reasonable” expectations of privacy in voice or writing samples, phone numbers, conversations recorded by concealed microphones, and automobile passenger compartments, trunks, and glove boxes.\(^{51}\)

Recently, the Court held in *Illinois v. Caballes* that the use of police dogs to sniff a car for drugs does not violate the privacy rights of stopped motorists.\(^{52}\) In explaining what may be viewed as a departure from earlier applications of Fourth Amendment privacy protection, Justice Stevens wrote:

\[\text{[T]he use of a well trained narcotics detection dog one that}
\]
\[\text{"does not expose noncontraband items that otherwise would}
\]
\[\text{remain hidden from public view," } \text{Place, 462 U.S. at}
\]
\[\text{707 during a lawful traffic stop, generally does not}
\]
\[\text{implicate legitimate privacy interests. In this case, the dog}
\]
\[\text{sniff was performed on the exterior of respondent's car while}
\]
\[\text{he was lawfully seized for a traffic violation. Any intrusion}
\]
\[\text{on respondent's privacy expectations does not rise to the level}
\]
\[\text{of a constitutionally cognizable infringement.} \]^\(^{53}\)

But the limits of the Fourth Amendment relative to personal information held in private hands are not new. Based on the Supreme Court's 1976 decision in *United States v. Miller*,\(^{54}\) it appears there is no reasonable expectation of privacy against government acquisition of information held by private entities (presumably including Internet companies and information brokers).\(^{55}\)

In the Internet context, the question is, to what extent does any constitutionally-rooted privacy right extend to the personal

---

53. Caballes, 543 U.S. at 409.
55. “Most pertinent to . . . government projects that could involve accessing data about U.S. persons from commercial databases, the Supreme Court held in 1976 in United States v. Miller, that there can be no reasonable expectation of privacy in objects or information held by a third party.” REPORT OF THE TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE APPOINTED BY THE U.S. DEPARTMENT OF DEFENSE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 22 (March 2004), http://www.cdt.org/security/usapatriot/20040300tapac.pdf.
information that is so key to transactions on the Web but that also may be said in virtually all instances to fall outside of the conception of "expectations of privacy" based on total secrecy? The answer to that question may depend on the degree to which there is recognition of a constitutionally based right of information privacy.

1. INFORMATION PRIVACY: CONSTITUTIONAL FOUNDATION

Like the right of privacy generally, the right of information privacy is implicit in several constitutional guarantees. The Supreme Court first acknowledged a constitutionally-based privacy interest in personal information in Whalen v. Roe. In Whalen, the Court upheld a statute requiring that centralized computer records be maintained on persons who purchased certain lawful drugs, for which there was also an illicit market, because it provided protections against disclosure. The disclosure protections were central to the Court's determination:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially harmful or embarrassing if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures . . . . [I]n some circumstances that duty arguably has its roots in the Constitution.

Indeed, Whalen provides one of very few examples of the Supreme Court's implicit recognition of a constitutionally based right of information privacy. In Whalen, the Court separated
the constitutional right to privacy into at least two interests: "the individual interest in avoiding disclosure of personal matters, and... the interest in independence in making certain kinds of important decisions." The former—avoiding disclosure of personal matters—has been widely acknowledged as the Court's definition of informational privacy. The vast majority of commentators have adopted a very similar definition, conceptualizing privacy as a right to control the flow of personal information.59

The interest in avoiding unwanted disclosure of personal matters is very much related to the interest in making important personal decisions or, stated more broadly, the interest in individual autonomy. Information privacy has been defined as "an individual's claim to control the terms under which personal

bankruptcy court's inclusion of a bankruptcy petition preparer's social security number (which was required to be provided) on public court documents. *Crawford*, 194 F.3d 954 (1999). There, the Ninth Circuit noted the Supreme Court's articulation of two kinds of constitutionally-protected privacy interests: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." *Id.* at 958 (citing Doe v. Attorney General, 941 F.2d 780, 795 (9th Cir. 1991) (quoting *Whalen*, 429 U.S. at 599-600)). The Ninth Circuit went on to say "the right of informational privacy, however, is not absolute; rather it is a conditional right which may be infringed upon a showing of proper governmental interest." *Crawford*, 194 F.3d at 959 (citing Doe v. Attorney General, 941 F.2d at 796).

Our precedents demand that we 'engage in the delicate task of weighing competing interests' to determine whether the government may properly disclose private information... Relevant factors to be considered include: the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access. *Id.* (internal citations omitted). The court went on to say that these factors are not exhaustive and that the relevant considerations may vary case by case and will depend on the overall context. *Crawford*, 194 F.3d at 959. Although the court recognized the constitutionally based interest in information privacy and that the disclosure of the complainant's Social Security number implicated that interest, it concluded that it did "not appear to constitute a more serious invasion of those interests than many other requirements imposed by government. Enhanced risk, in fact, obtains anytime the government requires an individual to deposit identifying information in the public record." *Id.* The court then said that to properly weigh the privacy interest, it must consider the probability of the identity theft feared. *Id.* The court distinguished a Social Security number from such sensitive information as HIV status, sexual orientation, or genetic makeup, which it described as "inherently sensitive or intimate information." *Id.* at 959-60. *See also* Doe v. City of New York, 15 F.3d 264 (2d Cir. 1994) (collecting cases and holding that there is a recognized constitutional right of informational privacy and that HIV status falls within that right).

information—information identifiable to the individual—is acquired, disclosed and used."\(^{60}\) The purposes of privacy protection are said to include "the promotion of liberty, autonomy, selfhood, human relations, and furthering the existence of a free society."\(^{61}\) Some commentators have said that "information privacy promotes distinct societal values by providing a context that allows, or creating the conditions in which, individuals may pursue their personal development"\(^ {62}\) and that privacy is "essential to the... maintenance of an autonomous self."\(^ {63}\) Given the importance of the rationales supporting privacy protection, the absence of a more explicit, robust, and coherent statement of information privacy protection is somewhat puzzling. As some commentators have noted, even though information privacy is not explicitly recognized as a constitutional right, given the imbalance in power between business and government entities with Internet access to personal information and individual subjects, information privacy should be viewed as "fundamental" and accorded greater legal protection to fill the "vacuum created between the constitutional principle and the inadequacies of statutory language."\(^ {64}\) Others have argued for a "limited" constitutional right to informational privacy that takes into account the competing interest in public access to government information.\(^ {65}\) There are those who go further and argue that more explicit, constitutionally-based information privacy protection should be afforded specifically to protect private information contained in public records.\(^ {66}\)


In addition to information privacy protections based on the federal Constitution as articulated in decisions such as Whalen v. Roe, some state constitutions arguably provide more robust or more explicit privacy protection against government intrusion.\(^67\) Again, however, the fit between privacy declarations and the practical ability to protect individual personal information is far from perfect. Moreover, constitutionally-based privacy protection generally runs only against government intrusion.\(^68\) In the context of the Internet, there is as much, if not more, concern about the private collection and aggregation of personal information as there is about government information-gathering.

2. INFORMATION PRIVACY PROTECTION AS AGAINST PRIVATE ACTORS

Other means of protecting privacy, primarily as against private actors, include the tort of invasion of privacy, state and federal consumer protection laws, and privacy protection statutes enacted to address a range of particular privacy concerns. These common law and legislative protections have proven to be blunt and largely inadequate tools for protecting individual informational privacy and security.

a. The Privacy Tort

The tort of invasion of privacy\(^69\) is defined differently from

\(^{67}\) Lin, supra note 66, at 1130-31. "Ten state constitutions [Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington] contain explicit provisions for privacy... Compared with their forty colleagues, these states have a 'clear opening for following an independent path.' Id. at 1130. However, Lin concludes that, on the whole, state constitutional protection for informational privacy has been "of little significance" largely because few information privacy cases have invoked these constitutional provisions. Id. at 1131.

\(^{68}\) But see Dorothy Glancy, At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 366 (2000): "[T]he California Constitution expressly guarantees 'an inalienable right of privacy.' Moreover, California's state constitutional privacy provision applies broadly to prohibit interference with privacy both by governmental and by private-sector invaders," (citing Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976)).

\(^{69}\) For a discussion about the origins of the privacy tort beginning with the seminal 1890 Warren and Brandeis law review article on privacy, see Ken Gormley, One Hundred Years of Privacy, 1992 WIS. L. REV. 1335, 1352-53:

The privacy of Warren and Brandeis was a tort notion, but it was meant to reflect a deeper instinct in the common law. It was meant to preserve an individual's "inviolable personality," a fragile and intangible thing, quite different than one's property or person, but essential to preserve a "civilized" and "cultured" society, particularly in an evolving American democracy which placed
state to state. As a general matter, traditional tort law privacy protection is based on four theories: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) misappropriation of name or likeness for commercial purposes, and (4) publicity that places another in a false light. \(^70\) While each of these theories might appear to provide protection against invasions of online privacy, as a practical matter, their utility in this context is very limited. For example, the intrusion upon seclusion privacy tort addresses "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns."\(^71\) For this privacy tort to apply, the invasion must be highly offensive to a reasonable person. Some courts have held that the tort does not apply where, as in most Internet transactions, the provision of the information is considered "voluntary" even when the uses to which the information is ultimately put may be unknown to the data subject. \(^72\)

Some commentators have argued that the tort involving public disclosure of private facts could be effective in preventing the publication of private or sensitive facts (such as a rape victim's name) over the Internet. \(^73\) However, there are constitutional limitations on imposing liability for disclosure of private facts that are (1) true and (2) available in court or public records. For example, in Cox Broadcasting Corp. \(v.\) Cohn, the Supreme Court held that the state may not impose sanctions on

---

a premium on the individual. Humankind's own inventiveness had created a new threat to solitude. The law, as it existed, was not equipped to deal directly with this new clash between citizen and environment. When the problem became acute enough, when society as a whole had been steeped in the consequences of its own ingenuity, a jolt occurred which was strong enough to create a new layer of law atop the old. The precise catalyst which thus introduced an explicit right of privacy in 1890, and thereafter led to its slow but steady acceptance throughout the United States, was the transformation of the American press, photography and the ability to engage in mass-circulation of information in a newly urbanized society.


71. RESTATEMENT (SECOND) OF TORTS § 652B.


By using the American Express card, a cardholder is voluntarily and necessarily giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.

73. Moira E. McDonough, Internet Disclosures of a Rape Accuser's Identity (Focus on the Kobe Bryant Case), 3 VA. SPORTS & ENT. L.J. 284 (2004).
the accurate publication of the name of a rape victim obtained from public records more specifically, from judicial records which are maintained in connection with a public prosecution and which themselves are open to public inspection.\textsuperscript{74} In addition, as Joel Reidenberg has noted, common law protection against public disclosure of private facts does not address privacy concerns for data collection or storage. To violate the right, the personal information must not generally be available or visible to the public and the information must relate to one’s ‘private life.’ In addition, the nature of the disclosure must be highly offensive to a reasonable person.\textsuperscript{75}

Reidenberg also identifies significant limitations in the application of the “intrusion upon seclusion,”\textsuperscript{76} “false light,”\textsuperscript{77} and “misappropriation”\textsuperscript{78} privacy torts in the context of commercial information processing and sharing.

\textsuperscript{74} Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 491 (1975). The result in Cox highlights the importance of court policies that, within judicial discretion, limit public access to information (such as the name of a rape victim) that though part of a public case is not itself of public concern such that it need be published to the world. See discussion infra Part III.


\textsuperscript{76} Reidenberg notes:

[An invasion of [the right of seclusion] can only result from the techniques used to collect personal information. Voluntarily disclosed personal information will be outside the scope of this right. Even if information is not voluntarily revealed, the particular means used to collect personal information must be highly offensive. Surreptitious or secret collections of personal information without notice or consent may be considered harmful by individuals, yet not rise to a sufficiently ‘objectionable’ level to meet the threshold standard. In any event, this right does not address other data protection practices such as the storage, use and disclosure of personal information.]

\textsuperscript{77} “The false light claim can be made only if there is a wide dissemination of misleading or erroneous personal information.” Id. at 225.

\textsuperscript{78} Reidenberg states:

“This protection against the misappropriation of one’s name may offer coverage for privacy concerns associated with some commercial data processing activities. The right originally emerged to address unauthorized endorsements in advertisements and commercial uses of photographs of individuals. Yet it is possible that this right could apply to ban certain uses, including dissemination, of personal information for commercial purposes without consent. However, privacy concerns associated with the collection of personal information notice and consent to data acquisition, unnecessary data compilation, and accuracy of data and the storage of personal information would be outside the scope of the misappropriation right.”

\textsuperscript{Id. at 225.}
In all of its iterations, the privacy tort is generally inadequate to protect privacy in the context of Internet transactions. This is because once a person gives information to another, he or she is said to have lost the ability to call that information "private." Internet transactions, by their very nature, involve the provision of information to another, rendering application of this tort virtually nonexistent in the Internet context. Each of the categories of privacy tort contains similar limitations when applied to the misappropriation and misuse of information obtained online, which is almost always information that the individual user has shared in another context.

b. Legislated Information Privacy Protection: A Disconnected Patchwork

The most promising vehicle for privacy protection is legislation that creates and enforces the rights of individuals to safeguard private or sensitive information. However, current legislative regulation of information privacy may best be described as an ad hoc patchwork of reactive laws and regulations rather than a cohesive scheme for the protection of personal information against unwarranted intrusions by private (or public) sector actors. While there is no shortage of legislation designed to address privacy concerns, very little of it has addressed effectively the concerns raised with respect to the collection, aggregation, and dissemination of individual personal information via the Internet.

Numerous federal laws have been enacted to respond to individual privacy concerns in one way or another. For example, the Electronic Communications Privacy Act ("ECPA"), an amendment to the federal wiretapping statute, is the primary federal legal protection against the unauthorized interception, accessing, use or disclosure of electronic communications while in transit or in storage. It has two substantive provisions that may apply in Internet privacy litigation: its prohibition on illegal interceptions of electronic communications (Title I of the ECPA - 18 U.S.C. 2511 et seq.) and its prohibition on illegal access to stored electronic communications (Title II of the ECPA – 18 U.S.C. 2701 et

79 For a discussion of the privacy tort in the Internet context, see Susan E. Gindin, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 SAN DIEGO L. REV. 1153, 1188-93 (1997).
ECPA is just one of many federal statutes aimed at addressing privacy concerns that have arisen as a result of advances in technology. Others include the Computer Fraud and Abuse Act,\textsuperscript{81} the Children’s Online Privacy Protection Act;\textsuperscript{82} the Cable Communications Policy Act,\textsuperscript{83} the Fair Credit Reporting Act,\textsuperscript{84} the Video Privacy Protection Act,\textsuperscript{85} and the Driver's Privacy Protection Act,\textsuperscript{86} to name just a few.

The DoubleClick litigation provides a good example of the shortcomings of existing privacy statutes in addressing core concerns about Internet privacy and security. In DoubleClick, plaintiffs alleged that DoubleClick was collecting information about the internet preferences of individual users (including

\begin{itemize}
  \item Seth Richard Lesser, \textit{Internet Privacy Litigation}, 788 PLI/Pat 189, 218 (2004).
  \item 18 U.S.C. §1030. According to commentators:
    \begin{quote}
      The Computer Fraud and Abuse Act was the first law to address computer crime with a specific statute. In 1990, Congress amended it to cover all computers used in interstate commerce or communications and 'to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce.’ The CFAA is a criminal statute which also provides a private, civil right of action for any violation of its terms.
    \end{quote}
  \item Lesser, \textit{supra} note 80, at 213.
    \begin{quote}
      The Children’s Online Protection Act of 1998 requires operators of Web sites directed to children under 13 to: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide parents the ability to review the personal information collected from their children; (4) provide parents the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child’s online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.
    \end{quote}
  \item Lesser, \textit{supra} note 80, at 207.
  \item 47 U.S.C. § 551 (2001) (prohibits a cable television company from using the cable system to collect personal information about its subscribers without their prior consent, and generally bars the cable operator from disclosing such data).
  \item 15 U.S.C. §§ 1681 et seq. (regulates the collection and use of personal data by credit reporting agencies).
  \item 18 U.S.C. § 2710 (2005) (prohibits videotape sales or rental companies from unauthorized disclosure of customer names and addresses, and the subject matter of their purchases or rentals for direct marketing use. Restricts videotape companies from disclosing personal data about customers without customers' consent or court approval).
  \item 18 U.S.C. § 272 (2005) (prohibits state motor vehicle departments from releasing personal information from driver's license and motor vehicle registration and title records).
\end{itemize}
clickstream data) and planned to combine this information with "a database of names, addresses, telephone numbers, retail purchasing habits and other personal information on approximately ninety percent of American households." According to Plaintiffs, this conduct violated the Electronic Communications Privacy Act ("ECPA"), Federal Wiretap Act, Computer Fraud and Abuse Act ("CFAA") and state law. Following a detailed analysis of each statute's applicability, the court determined that the plaintiffs' complaint failed to state a cause of action under any of them. Addressing the plaintiff's ECPA claim, the court acknowledged that "Internet access is the relevant electronic communications service" and that "web sites are 'users' under the ECPA." It then concluded that "[a]ll of the communications DoubleClick has accessed through its cookies have been authorized or have fallen outside of [ECPA] Title II's scope." The court focused on the relationship between DoubleClick and its affiliated Web sites and found that the Web sites had consented to DoubleClick's interception of plaintiff's communications. The court then said that "Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such."

With respect to the Wiretap Act, the court read the relevant portion of the Act to require an element of "tortious" or "criminal" mens rea and found none with respect to DoubleClick's actions. The court also found that plaintiffs failed to allege facts that would meet the Consumer Fraud and Abuse Act's damages threshold. Having dismissed the federal claims, the court declined to exercise supplemental jurisdiction over the remaining state law claims. Thus, notwithstanding pleading under several

88. Id. at 499.
89. In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d at 526.
90. Id. at 508.
91. Id.
92. Id. at 510.
93. Id.
94. In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d at 510.
95. Id. at 515. "DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites." Id.
96. Id. at 526.
97. Id. The state law claims were pursued by several state attorneys general. "In
federal statutes apparently designed to protect the privacy and security of electronic communications, the DoubleClick plaintiffs were unable to successfully plead a federal cause of action to address the unauthorized aggregation and sharing of personal information. 98

In some instances, State consumer protection law has provided more effective remedies for Internet overreaching than some of the federal statutes that appear designed protect Internet privacy. For example, many state attorneys general have used consumer protection statutes aimed at “deceptive acts and practices” to prevent Internet Service Providers (“ISPs”) from misleading the public about the collection and use of the information they provide over the Internet. 99 In the late nineties this was done through the enforcement of privacy policies state attorneys general sued ISPs that failed to adhere to the terms of their privacy policies’ representations that personal information would not be shared with third parties. Unfortunately, many ISPs decided that their interest in trading in individual information was more valuable than representations not to share personal information and so they simply changed their privacy policies to notify users that their information would be shared with third parties. This left little room for enforcement based on deceptive practices and, as a practical matter, left Internet users, who either did not read the privacy policies or assumed that the existence of a privacy policy would be protective, virtually clueless about the uses of their personal information and with scant means of preventing unwanted uses.

August 2002, the New York and ten other Attorneys General settled an extensive investigation into the privacy practices of third party marketer and ad server DoubleClick . . . ” Kenneth M. Dreifach, Data Privacy, Web Security, and Attorney General Enforcement, 828 PLI/Pat 401, 414-15 (2005). The Assurance required DoubleClick to disclose its activities in a privacy policy, and to monitor these disclosures; to segregate data acquired through its advertising/contracting from its profiling functions; to submit to outside privacy audits over 4 years’ and to pay the collective states $450,000. Id. at 415.

98. See also In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 12-15 (D. Mass 2002) (finding that a company’s use of Web site tracking devices to collect personal data from visitors to pharmaceutical Web sites did not violate the federal wiretap Act, ECPA, or the CFAA.)

Despite the challenges created by the limitations in many of the statutes enacted to protect specific aspects of individual privacy, Congress continues to propose and enact legislation in response to narrow, specific privacy concerns that come to the public's attention rather than re-thinking individual privacy protection more broadly. Some observers attribute this ad hoc, reactive and narrowly targeted approach to First Amendment concerns about the free flow of information coupled with the business community's preference self-regulation. The limitations of existing privacy legislation may be attributed in part to the narrow interests of elected legislators in responding to public outcry while at the same time not doing too much to upset the powerful business interests that have a large stake in the trade of detailed individual information.

Whatever the reason, the protection of information privacy has been left to vague (and arguably diminishing) constitutional protections against government intrusion, common law tort actions that are largely ineffective, and a patchwork of state consumer protection laws and narrowly targeted state and federal laws addressing very specific aspects of information privacy protection. Despite a long list of federal and state laws addressing privacy, gaping holes remain in the protection of individual privacy in almost every context. Furthermore, the seemingly endless list of privacy legislation proposed over the last five years seems unlikely to respond effectively to these concerns given the reluctance of lawmakers to address individual privacy at a broad policy level. Still, the most appropriate place for government intervention in preserving and protecting privacy is

100. See, e.g., S. 1789, 109th Cong. § 103 (2005) (amending FCRA to impose a fraud alert system upon credit reporting agencies); see also Epic Bill Track (2005), http://www.epic.org (providing a list and description of the bills currently before congress affecting internet privacy); Dreifach, supra note 97, at 420-21 (discussing Internet privacy legislation in the 109th Congress).

101. See, e.g., The Florida Star v. B.J.F., 491 U.S. 524 (1989) (holding that imposing damages on a newspaper for publishing a rape victim's name pursuant to a state statute prohibiting such publication violated the First Amendment). As one commentator has noted:

[L]egislatures respond only to specific issues. Legal standards are justified only where targeted for a particular problem: therefore, standards often develop on an ad hoc basis, by reaction to public scandals. Examples include the protection of video rental records following the disclosure of records for a nominee to the U.S. Supreme Court and the Fair Credit Reporting Act, which was enacted in response to consumer horror stories about dealing with credit reporting agencies.

through legislation.

Fortunately, some promising legislative proposals aimed at protecting privacy more comprehensively and practically have begun to appear in response to broadening concerns about hackers acquiring vast amounts of personal information. For example, a recent California law requiring information brokers to disclose to customers security breaches, resulting in the unauthorized dissemination of their personal information, has shed light on numerous data breaches and prompted calls for similar legislation on the federal level. United States Senator Dianne Feinstein has introduced a similar breach notice law on the federal level that would provide consumers nationwide with notice of security breaches that might involve their personal or sensitive information.

While much of this legislation, like earlier privacy legislation, is reactive, current legislative proposals are beginning to focus on placing some measure of power in the hands of data subjects, an approach that is more likely to be effective in addressing the core concerns about Internet privacy. In contrast to much of the earlier privacy legislation which focused on the particular kind of information at issue or the methods of collection or transfer employed, some of the current proposals focus on informing and involving the data subjects in more meaningful ways.

---

102. CAL. CIV. CODE § 1798.29 (West 2005).
105. See supra note 103 (discussing the ChoicePoint breach).
106. Such proposed legislation comes closer to effectuating the fair information principles of notice, choice, access, and security, acknowledged by the FTC and others as critical to effective Internet security. See FTC REPORT, supra note 33, at 3-4.
II. THE INTERNET PROMISES GREATER PUBLIC ACCESS TO COURT RECORDS AND GREATER TRANSPARENCY OF COURT FUNCTIONS, BUT HIGHLIGHTS THE PERCEIVED DIFFICULTY IN PROTECTING INDIVIDUAL PRIVACY WHILE PREVENTING GOVERNMENT SECRECY

Against a backdrop of intense concern about information privacy protection, it is possible to lose sight of the Internet's promise of greater transparency. To some observers, the Internet promises to shed ever greater light on government operations, allowing the public to obtain information, participate in politics and government affairs, and engage in oversight of government as never before. For example, Internet access now allows people to obtain information about legislation, rulemaking, and budget decisions that traditionally have been difficult to locate. E-government acts have made it easier for citizens to gain access to government information and services, such as driver's license applications and tax filings. The Internet has improved the citizen oversight function in many ways by providing online access to information about campaign contributions, the voting records of representatives, and yes, court indices, calendars, and decisions.

107. See Solove, supra note 27, at 1173. Solove observes that:
There are at least four general functions of transparency: (1) to shed sunshine on governmental activities and proceedings; (2) to find out information about public officials and candidates for public office; (3) to facilitate certain social transactions, such as selling property or initiating lawsuits; and (4) to find out information about other individuals for a variety of purposes.

Id.

108. As a 2003 Report to Congress on Implementation of the E-Government Act explains:
E-Government is the use of information technology (IT) and the Internet, together with operational processes and people needed to implement those technologies, to deliver services and programs to constituents, including citizens, businesses and other government agencies. E-Government improves the effectiveness, efficiency and quality of government services.


A. **Public Access to Government Records Is Generally Viewed as an Antidote to Government Secrecy**

In the context of public records, some argue that restricting access in the service of privacy, is likely to yield something worse than the sharing of too much individual information: increased government secrecy. To these observers, overzealous efforts to protect so-called “private” information contained in public records, will only serve to create more secrecy in government operations without necessarily improving privacy protection. The government will continue to amass vast amounts of information about its citizens, but individuals will be less able to observe government functions. The concern about government secrecy, particularly with respect to the immense amount of information being gathered about individuals, raises concerns about government control, manipulation, and punishment, and impairing individual autonomy through boundless, unseen surveillance:

we can see the primary principle of the Panopticon in operation. The Inspector, now the Bureaucrat, scans the subjects, now the Society, rendered as transparent as possible to his gaze. The transparency, however, is not two-way, as the state jealously guards itself through administrative secrecy. It appears to the subjects as an impenetrable object (and separated as administration is from politics, not directly accountable to democratic voters.) Coercion lurks in the background of course, as an underlying sanction encouraging compliance with a state which has a high likelihood of seeing and noting infractions of its rules.

This vision of the panopticon operated by the secret and

---


113. As Dorothy J. Glancy explains: Bentham's concept of a panopticon prison made each prisoner's every movement continuously visible to guards who could watch all of the prisoners all of the time. Bentham noted that in practice it would not be necessary to have guards actually watch each prisoner at every moment. Simply the potential for complete
coercive state or Bureaucrat stands in contrast to efforts by courts to provide greater access and transparency to public court records by making them available over the Internet. However, it is not an unrealistic assessment of some of the operations of government particularly in the context of law enforcement following the terrorist attacks of September 11, 2001. Indeed, the combination of government collection of vast amounts of individual personal information and government secrecy about the contents and uses of that information present a threatening, autocratic, and anti-democratic vision of government that calls to mind Kafka’s The Trial, Orwell’s 1984, and Bentham’s Panopticon.

The recent case, Doe v. Ashcroft, provides an extreme example of government secrecy in the context of Internet information gathering. In Doe, an Internet service provider (ISP) brought a constitutional challenge against 18 U.S.C. § 2709, a statute authorizing the Federal Bureau of Investigation to compel communications firms, such as ISPs to produce certain customer records whenever the FBI certifies that those records are relevant to an authorized investigation to protect against terrorism. The

and continuous visibility would cause each prisoner to watch himself all the time. Such a system would, Bentham argued, give the state even more power over prisoners than keeping the prisoners bound in chains. In short, the panopticon was designed to give authorities intense control over prisoners. Concerns about abject conformity and warped human personalities that could result from such a dystopian everyone-is-visible-all-the-time regime was, of course, part of the searing image of an all-seeing Big Brother in George Orwell’s novel, 1984.


116. Ironically, “Section 2709 was enacted as part of Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), which sought to ‘protect privacy interests’ in ‘stored wire and electronic communications’ while also ‘protecting the Government’s legitimate law enforcement needs.’” Id. at 480. Congress looked to the Right to Financial Privacy Act ("RFPA") of 1978 as a model for the ECPA. Id. The RFPA was passed primarily in response to cases like United States v. Miller, 425 U.S. 435 (1976), which held that customers of a financial institutions could not bring a Fourth Amendment claim to contest government access to financial records. Id. “In passing Title II of the ECPA eight years later, Congress feared that customers of electronic communications services would... find little Fourth Amendment protection from Government access to their records, thus creating the need for privacy legislation.” Id. at 481.

FBI's requests take the form of national security letters ("NSLs"), which bar the recipient ISPs from ever disclosing to anyone (presumably, by the statute's terms, including their lawyer) that they have received such letters. The ISP, ("Doe"), challenged these national security letters as unconstitutional on their face and as applied, in that they give the FBI "extraordinary, unchecked power to obtain private information without any form of judicial process" (in violation of the First, Fourth, and Fifth Amendments) and that the statute's absolute nondisclosure provision "burdens speech categorically and perpetually, without any case-by-case judicial consideration of whether that speech burden is justified." In determining that the NSLs were unconstitutional, District Judge Victor Marrero noted that not only did they violate the rights of the ISP, but they also could be used to infringe ISP subscribers' rights. The district court based its holding on Supreme Court doctrine providing that "compelled disclosure of affiliation with groups engaged in advocacy" amounts to a "restraint on freedom of association" where disclosure could expose the members to "public hostility." The district court's description conjures the principle of the panopticon at work:

For example, the FBI theoretically could issue to a political campaign's computer systems operator a §2709 NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL under §2709 to discern the identity of someone whose anonymous online web log, or "blog," is critical of the Government. Such inquiries might be beyond the permissible scope of the FBI's power

(a) Duty to provide. A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section . . . . (c) Prohibition of certain disclosure. No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

119. Id.
120. Id. at 506.
121. Id. at 507 (citing NAACP v. Alabama, 357 U.S. 449 (1958) (holding that state could not compel association to produce records identifying its members and agents without entailing a substantial likelihood of offending and infringing upon the freedom of association)).
under § 2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment. These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.\(^{122}\)

Thus, *Doe v. Ashcroft* presents an egregious example of secret and pervasive government information-gathering without any public or legal oversight. In that case, the secrecy was the function of the Executive Branch's issuance of national security letters, and the remedy for such secrecy was with the courts. Government record-keeping and information-gathering takes a variety of forms and results in the accumulation of vast amounts of personal information.\(^{123}\) Often, it is said, the best check on government abuse of its authority in the context of societal surveillance is to provide public access to, and judicial oversight of, these governmental activities. As Judge Marrero noted in *Doe v. Ashcroft*:

> In general, as our sunshine laws and judicial doctrine attest, democracy abhors undue secrecy, in recognition that public knowledge secures freedom. Hence, an unlimited government warrant to conceal, effectively a form of secrecy per se, has no place in our open society. Such a claim is especially inimical to democratic values for reasons borne out by painful experience. Under the mantle of secrecy, the self-preservation that ordinarily impels our government to censorship and secrecy may potentially be turned on ourselves as a weapon of self-destruction."\(^{124}\)

Indeed, an important counterpoint to concerns about individual privacy in the context of placing court records on the Internet is the competing and legally recognized interest in

---


123. See, e.g., Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (attempting to define a theoretical approach to strike an "appropriate balance between privacy and effective law enforcement"). *Id.* at 1088.

government transparency—in providing public access to information about government functions. This interest in transparency is deemed particularly potent in the context of court proceedings and records largely because of the important role the courts play in ensuring adherence to law and securing fundamental constitutional rights.

Proponents of broad Internet access to court records say such access will serve this interest in transparency. Internet access to court records can serve to de-mystify court operations, provide public information and oversight of the judicial function, and support accountability and public confidence. In the context of court records, some supporters view Internet access as a window on a fundamental public process that had been "practically obscure." In this way, providing broad Internet access to court records could be seen as a move away from the negative notion of government as the unseen, secret collector of information and as a way to distinguish the courts from government institutions that collect, disseminate, and use information in secret to exert power over individuals and society.

Yet as noted below, competing interests confront court systems, as obvious tensions exist between the right of openness, on the one hand, and concerns about privacy, security, fairness, and court administration, on the other. Therefore, although the impulse toward greater openness and public access is to be welcomed and encouraged, a completely unqualified policy of open access is not a viable choice for courts. At the same time, courts must carefully consider how they might develop policies designed to provide greater access for the appropriate purposes of providing public information, oversight, and accountability, while protecting legitimate interests in individual privacy and security and fostering effective judicial administration.

B. THE LAW RECOGNIZES A CONSTITUTIONALLY-BASED, THOUGH QUALIFIED, RIGHT OF PUBLIC ACCESS TO COURT RECORDS

A long recognized presumption of public access to court records exists in the common law. While "[t]here is not yet any

125. See, e.g., Reporters Committee for Freedom of the Press Homepage, http://www.rcfp.org; see also infra note 134.

126. See, e.g., Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) (plurality concluding that the right of the press and the public to attend criminal
definitive Supreme Court ruling on whether there is a constitutional right of access to court documents and if so, the scope of such a right[,]” the common law presumption in favor of access to court records is fairly strong.127 The Supreme Court articulated this common law right of public access to court documents in Nixon v. Warner Communications: “It is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents.”128 This right is designed to promote public confidence in the judicial system and to diminish the possibilities for injustice, perjury, and fraud.129 However, as the Court noted in Nixon, the “right to inspect and copy judicial records is not absolute. Every court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes.”130 To determine whether access to a judicial document legitimately may be denied, the court must engage in a balancing test, inquiring whether the right of access is outweighed by interests favoring non-disclosure.131

Some argue that the presumption of public access to court records is constitutionally based and can only be overcome by the demonstration of a compelling interest.132 Those who make this

---

128. Id.
129. See, e.g., Richmond Newspapers, Inc., 448 U.S. at 595.
130. Nixon, 435 U.S. at 598.
131. Nixon, 435 U.S. at 602; see also United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997) (explaining that presumption in favor of availability exists).
argument often cite the Supreme Court’s decision in *Richmond Newspapers v. Virginia* as support. However, *Richmond Newspapers* stands for the “right of the public and the press to attend criminal trials” and does not extend to a constitutionally grounded right of access to all court records and information. Yet, as Arthur Miller has observed:

>[A]n intense, nationwide campaign is underway to create a ‘presumption of public access’ to all information produced in litigation that would seriously restrict the courts’ traditional discretion to issue protective and sealing orders shielding litigants’ documents from view . . . . [T]he more extreme proponents of increased public access seek to give the halls of justice walls of glass, so that nothing is withheld from the public eye, no matter how private, insignificant, or inaccurate it might be.  

These same proponents have made the argument that there is a constitutionally based right of public access to court records and public documents in the context of shaping court policies regarding Internet access to court records. Advocates of

---

133. In *Globe Newspaper Co.*, a case overturning a Massachusetts law that was interpreted to require exclusion of the press and public during testimony of minor victims of alleged sex offenses, the United States Supreme Court expressly reaffirmed that Richmond Newspapers dealt only with that access to criminal trials. 457 U.S. at 611. Two later decisions, *Press-Enterprise Co. v. Superior Court I*, 464 U.S. 561 (1984) (upholding access to voir dire examination of potential jurors in a criminal trial absent findings that would justify closure in a particular case) and *Press-Enterprise Co. v. Superior Court II*, 478 U.S. 1 (1986) (allowing further press access to transcripts of a preliminary hearing in a criminal case), extended the *Richmond Newspapers* holding somewhat, but only in the context of a criminal trial. See Comments of the Commercial and Federal Litigation Section of the New York State Bar Association to the Commission on Public Access to Court Records (July 2003) available at http://www.nycourts.gov/ip/publicaccess/links.shtml.


Many members of the Advisory Committee expressed the view that the presumption of openness is constitutionally based, requiring a “compelling interest” to overcome the presumption. Other members expressed the view that the law in this area is evolving. The Joint Court Management Committee of CCJ and COSCA took the position that, because the issue may well come before courts of last resort, the CCJ/COSCA Guidelines should not take a position as to the applicable legal standard.

*Id.*
completely unrestricted Internet access to court records have made their point quite forcefully to court systems in the process of developing policies to balance public access with privacy, security, court administration and other concerns.136

For example, the Reporters Committee for Freedom of the Press advocates for virtually no overarching court policy to address privacy, security or administrative concerns when providing online access to court records beyond a very narrow application of the case-by-case analysis in which judges already engage (most often, only when prompted by the parties). The Reporters Committee is among the leading advocates of the view that the public right of access to court records is constitutionally based and near absolute. Yet, as a legal and practical matter, the right of access in the context of court records must be limited. This limitation is not only necessary because of "vague" interests in individual privacy, but also to ensure that access to court records serves appropriate public functions, including not only privacy and security, but also the sound and efficient administration of justice. As Daniel Solove notes:

[E]ven under an expansive view, the right to access does not apply to efforts to restrict the access to personal information for particular uses. When public records illuminate government functioning, access to government records is

136. For example, the Reporter's Committee for Freedom of the Press issued the following talking points regarding online access to court records:

Here are the key considerations for openness advocates to make when considering the drafting of a court access policy:

Information available at the courthouse should be available online. Allowing access to particular records only at the courthouse means courts believe in public access only when it's not practical.

The best way to accommodate legitimate privacy interests is to allow judges to make case-by-case decisions to restrict access to particular information in files, if the requestor can demonstrate a compelling need.

Electronic access rules should not impose such a burden on court personnel that individual courts will soon have backlogs of records waiting for "approval" before being made available online.

Records made available electronically for judges and lawyers should be available to the public, for the same reasons judges and lawyers find this method of access beneficial.

Electronic access ensures that the public and the news media can oversee how justice is administered like never before.

"Privacy" is a vague interest that, without attempts to concisely define what it means, cannot justify barring access to a wide range of information that is important to the public understanding of the court system.

generally consistent with the rationale for the First Amendment right to access. However, the grand purposes behind the right to access are simply not present in the context of much information gathering from public records today . . . . In fact, the Constitution does not simply require open information flow; it also establishes certain responsibilities for the way that the government uses the information it collects.\textsuperscript{137}

Courts have long exercised supervisory power over their records to avoid the use of court records for improper purposes. This power is consistent with other governmental efforts to balance the interest in public access to government with competing interests in individual privacy, security, and governmental administration. For example, the federal Freedom of Information Act\textsuperscript{138} and its state law counterparts, while designed to encourage broad public access to government information "to ensure an informed citizenry, [which is] 'vital to the functioning of a democratic society,'"\textsuperscript{139} include several exemptions that mirror the concerns raised in the context of court records. On the federal level "[t]he Freedom of Information Act ("FOIA") and Privacy Act . . . do not apply to the judicial branch and do not govern access to case file documents."\textsuperscript{140} Most state courts also are not subject to state freedom of information laws. However, many court systems have statutory, regulatory, and/or common law counterparts that favor public access, but permit nondisclosure for "good cause" shown\textsuperscript{141} sometimes articulating a

\textsuperscript{137} Daniel J. Solove, supra note 27, at 1203-04.
\textsuperscript{140} Robert Deyling, Privacy and Access to Electronic Case Files in the Federal Courts 5, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, OFFICE OF JUSTICE PROGRAMS (Dec. 15, 1999), http://www.uscourts.gov/privacyn.pdf (citing 5 U.S.C. §§ 551(1)(B) & 552(f)); United States v. Frank, 864 F.2d 992,1013 (3d Cir. 1988) (stating that certain federal disclosure statutes "by their terms do no apply to the judiciary"); Warth v. Department of Justice, 595 F.2d 521, 522-23 (9th Cir. 1979) (holding that "the provisions of the FOIA impose no obligation on the courts to produce any records in their possession").
\textsuperscript{141} For example, Section 216.1(a) of the New York Rules of Court provides that:

\[e]xcept where otherwise provided by statute or rule, a court shall not enter an order in any action . . . sealing the court records, whether in whole or in part, except upon a written finding of good cause, which shall specify the grounds thereof. In determining whether good cause has been shown, the court shall consider the interests of the public as well as of the parties.

very strong presumption favoring openness.\textsuperscript{142} Notwithstanding this presumption of openness, several courts have been criticized for erring on the side of closure and permitting secrecy in the settlement of cases involving issues of public safety.\textsuperscript{143}

C. Concerns About Secrecy Complicate Court Efforts to Balance Public Access and Privacy When Placing Court Records on the Internet

Concerns about shielding from public view records and information which are in the public interest have further complicated the access/privacy debate regarding online court records. As advocates of privacy, domestic violence prevention, consumer protection interests, as well as those representing clients in matrimonial\textsuperscript{144} and juvenile cases,\textsuperscript{145} urge courts to shield certain classes of information in court records from broad Internet access, efforts are still being made to curtail courts’ use

\textsuperscript{142} See, e.g., Rule 243.1(d) of the California Rules of Court, stating that:

\[\text{[t]he court may order that a record be filed under seal only if it expressly finds facts that establish: (1) [t]here exists an overriding interest that overcomes the right of public access to the record; (2) [t]he overriding interest supports sealing the record; (3) [a] substantial probability exists that the overriding interest will be prejudiced if the record is not sealed (4) [t]he proposed sealing is narrowly tailored; and (5) [n]o less restrictive means exist to achieve the overriding interest.}\]

\textsc{Cal. Rule of Court 243.1(d)} (West 2005).

\textsuperscript{143} Compare Elizabeth E. Spainhour, \textit{Unsealing Settlements: Recent Efforts to Expose Settlement Agreements That Conceal Public Hazards}, 82 N.C. L. REV. 2155 (2004) (arguing that protective orders appended to private settlements which conceal public hazards should be declared void as a matter of public policy), with Laurie Kratky Dore, \textit{Settlement, Secrecy, and Judicial Discretion: South Carolina's New Rules Governing the Sealing of Settlements}, 55 S.C. L. REV. 791 (2004) (suggesting that judicial involvement regarding access to documents may be more important as regards pre-trial discovery and documentary evidence than sealing terms of a settlement); see also Stephanie S. Abrutyn, \textit{Commentary, Courts Are Just as Guilty in Church Coverup}, HARTFORD COURANT, May 26, 2002 at C1, \texttt{http://www.courant.com}; Mike France, \textit{The Hidden Culprit: The U.S. Legal System}, \textsc{BusinessWeek Online}, Sept. 18, 2000, \texttt{http://www.businessweek.com/2000/00_38/b3699193.htm} (discussing public access to civil litigation when serious public safety concerns are involved).

\textsuperscript{144} See Laura W. Morgan, \textit{Strengthening the Lock on the Bedroom Door: The Case Against Access to Divorce Court Records Online}, 17 J. AM. ACAD. MATRIMONIAL LAW 45 (2001) (arguing that divorce records and files should be presumptively private, as compared to other proceedings).

of sealing orders. These efforts to limit the use of sealing orders focus on concerns about denying the public access to information about court cases addressing potential hazards that would otherwise be brought to light, to the benefit of the broader society. The concern about "secret settlements" stems from truly troubling incidents, such as the use of court-sanctioned sealing of litigation as part of settlement agreements to conceal Bridgestone tire defects that were responsible for numerous accidents, as well as to shield from the public a pattern of child sexual abuse allegations against priests. Indeed, over the last few years, a number of states have enacted or considered legislation which curtails the ability of courts to seal settlement records in cases that involve issues of public safety.

The impulse to limit the sealing of court records and settlement information in cases involving issues of public concern is a sound one. Before state and federal legislators adopt new legislation to limit or eliminate judicial discretion over closure of court records, however, those legislators should examine the degree to which existing "good cause" requirements (in conjunction with judicial education) sufficiently address the concern about secret settlements or the excessive use of sealing.

The question here, as with policy development regarding Internet access to public court records, is whether existing structures, which balance competing interests in permitting or limiting public access, should be examined and improved upon before the legislators (or courts) impose new rules.

146. See Dore, supra note 143, at 792-93.
147. See Spainhour, supra note 143, at 2156-57 ("Nearly twenty states now have laws affecting settlement confidentiality in varying forms and degrees. The trend toward addressing hidden dangers in litigation documents continues.").
148. As Arthur Miller notes, FED. R. CIV. P. 26(c) and state counterparts contain a "good cause" requirement prior to the issuance of protective orders. Arthur R. Miller, Confidentiality, Protective Orders, and Public Access to the Courts, 105 HARV. L. REV. 427, 467 (1991) (arguing that laws prohibiting secret settlements "impose a superfluous and inordinate work burden on the courts"). The requirement of a "good cause" showing, effectively enforced, may be sufficient to address the concerns about secret settlements without going too far in tying judges' hands. See also George Carpinello, Public Access to Court Records in New York: The Experience Under Uniform Rule 216.1 and The Rule's Future in a World of Electronic Filing, 66 ALB. L. REV. 1089 (2003) (making similar arguments regarding New York's rule requiring a "good cause" showing before court case records may be sealed).
149. See, e.g., Joseph D. Steinfeld, Eve Burton, et al., Recent Developments in The Law of Access, 726 PLI/Pat 7, 52-53 (2002) ("When should the identities of persons involved in [clergy sexual abuse] cases be kept secret? . . . To answer this question, the court used a good cause impoundment analysis, identifying as critical factors the
To the extent that efforts to prevent courts from exercising broad discretion to seal court records might appear to be on a collision course with proposals to limit public access to private or sensitive information contained in court records, a few points are worth noting. First, both impulses are based on the interest in ensuring public access to information that serves the interests for which public access is required: to inform and educate the public about the workings of the courts, and as a mechanism for oversight and accountability. Judges and court policy-makers, seeking to balance public access with competing interests must bear in mind not only individual interests in privacy and security, but also the effect of their actions on the sound administration of justice. In the context of sealing records, there are those who have argued that, if certain civil cases in which the parties seek to preclude public access are kept open to public scrutiny, certain litigants' interests will be impaired so that litigants may resort to private fora rather than the public court system to resolve disputes.

On the other hand, others argue that once people avail themselves of the court system to resolve disputes, they have acquiesced to having the dispute resolved in a public forum, that is, to having all that is revealed about them in the proceeding exposed to the world.\footnote{150} Not everyone in court, however, appears there voluntarily—people required to appear in court involuntary may argue that they did not chose to participate in a dispute addressed in a public forum. Because this is true for at least half of all civil litigants (and, it is fair to say, all of those in criminal court), courts should not glibly take the position that everyone appearing in court acquiesces to being there and to subjecting their disputes to public scrutiny.

At the same time, judges should be made aware that it is not appropriate to seal a court record simply on the agreement of the parties. This standard regarding private agreements is applicable when a party's personal, business, or reputational interests are at stake, absent a showing that no public interest in the information exists or that the litigants' competing concerns outweigh the public interest in the information.\footnote{151} The mere

\footnote{150} See, e.g., Miller, supra note 134, at 466.
\footnote{151} See David S. Sanson, The Pervasive Problem of Court-Sanctioned Secrecy and
threat that litigants will go elsewhere is not enough to warrant the wholesale sealing of records, though courts (and legislatures) should be cognizant of the possible ancillary effects of their actions with respect to sealing.

Second, the call to protect certain data elements, documents, and cases, which are clearly not in the public's interest, or cases in which there is a showing that a release would cause significant harm to litigants, witnesses, or others, is not necessarily inconsistent with a call to limit pro forma sealing of settlements or of court documents upon the request of one party or the agreement of both parties. The critical difference between much of the information sought to be shielded in the Internet context and the information that was shielded in the context of complained-of secret settlements is that the former generally does not contribute to stated interests in transparency, while the latter does.

The difficulty for court systems lies in the fact that many instances exist in which the subject matter of a case includes elements of both private, sensitive information and information arguably related to the public's interest in maintaining judicial oversight. Some examples include: juvenile cases involving on one hand the concern of guarding information pertaining to minors, and on the other a competing interest in supervising the justice system's treatment of juveniles\(^\text{152}\) and medical malpractice

---

\(^{152}\) See, e.g., Barry C. Feld, The Constitutional Tension Between Apprendi and McKeiver: Sentence Enhancements Based on Delinquency Convictions and the Quality of Justice in Juvenile Courts, 38 WAKE FOREST L. REV. 1111, 1183, n.234 ("Policies on access to juvenile records pose a conflict between the rehabilitative goals of the juvenile court and the public safety interests [in] identifying career criminals"); see also NATIONAL CENTER FOR STATE COURTS, PUBLIC ACCESS TO COURT RECORDS: IMPLEMENTING THE CCJ/COSCA GUIDELINES FINAL PROJECT REPORT 30 (Oct. 15, 2005), http://www.ncsconline.org/WC/Publications/Res_PriPubAccCrtRcrds_FinalRpt.pdf. There are special issues involved in family court records that suggest that some information be kept private regardless of their [sic] form (paper or electronic):

- Sensitive information about individuals contained in the records (including mental health and other reports);
- The danger of identity theft due to high amount of personally identifiable information contained in the records (e.g., financial statements in custody and support filings);
cases, in which personal medical information (normally considered confidential), is central to the outcome of the case and may be necessary to know in making a determination regarding the appropriate outcome of such cases. In these circumstances, courts are faced with very difficult choices. Some court systems need not address these issues because certain classes of cases such as juvenile, matrimonial, and family law cases are closed by statute or court rule. Others address the tension between public interest and privacy concerns on a more case by case basis. On balance, determinations regarding when and to what degree "good cause" exists to close a courtroom or to seal a court document appropriately belong with the courts.

Viewing the question from a separation of powers and checks and balances perspective, the judiciary, given its role as the interpreter of the law, its supervisory power over court records, and its responsibility for the sound administration of justice, should retain discretion in addressing tough cases regarding whether and when matter in court proceedings should be shielded from public view. Should judges and court administrators fail to

---

The therapeutic role of the court could be challenged if participants don't trust the security of the disclosures made there due to inadequate privacy protections;

The historical "family privacy" value in American society has some weight that needs to be balanced here.

NATIONAL CENTER FOR STATE COURTS, PUBLIC ACCESS TO COURT RECORDS: IMPLEMENTING THE CCJ/COSCA GUIDELINES FINAL PROJECT REPORT at 30.

153. See, e.g., Report to the Chief Judge of the State of New York by the Commission on Public Access to Court Records supra note 3 at 20-24; Mary Jo Brooks Hunter, 1997 Special Report: Minnesota Supreme Court Foster Care and Adoption Task Force, 19 HAMLIN J. PUB. L. & POL’Y 1, 165 ("Except with regard to the records in certain juvenile offender cases, none of the records of the juvenile courts and none of the records relating to an appeal from a non-public juvenile court proceeding, except the written appellate opinion, are open to public inspection"); Daniel Morman & Sharon R. Bock, Electronic Access to Court Records, A Virtual Tightrope in the Making, 78 Fla. B. J. 10 (Nov. 2004) (discussing objections of family lawyers to placement of electronic court records on the Internet). But see IMPLEMENTING THE CCJ/COSCA GUIDELINES, supra note 149, at 32. ("While the common historical assumption has been that dependency and delinquency proceedings should be closed, and the court records of those proceedings similarly unavailable to the public, this assumption has been changing in recent years . . . . In only 21 jurisdictions [abuse and neglect] proceedings closed for all cases").

154. Bryan Morrison, Note, To Seal or Not to Seal? That is Still the Question: Arkansas Best Corp. v. General Elec. Capital Corp., 49 Ark. L. REV. 325, 328-29 (1996) ("Courts generally have determined that when faced with a sealing issue, no bright line public access rule should apply; rather, the decision should be made on a case-by-case basis.").

155. See Miller, supra note 134, at 501.
exercise that discretion in a manner consistent with the public interest, the threat of legislation limiting that discretion should serve as a wake up call and perhaps ultimately an absolute restriction. However, before such legislation is enacted, careful consideration should be given to strengthening and clarifying existing frameworks for balancing access, privacy, security, and judicial administration.  

Requests to limit access to personal identifying information in public court records posted on the Internet and requests to seal cases where the litigants agree to keep actual and potential public hazards confidential can be distinguished in court policies regarding both Internet access and elaboration of the “good cause” requirement for sealing court records. As noted below, an important component of court systems’ work regarding these issues should involve judicial and public education that focuses on the purposes for which courts and court records are presumed open and on the particular concerns that warrant closure. Attention also should be paid to the courts’ roles in interpreting law and administering justice versus the roles and responsibilities of the other coordinate branches. In both instances, however, existing frameworks for balancing public access and privacy and confidentiality should be considered and utilized (or perhaps modified) before any broad legislative or policy requirements are added.

III. THE COMBINATION OF PRIVATE AND PUBLIC SECTOR INFORMATION GATHERING, AGGREGATION, AND DISSEMINATION IMPACT PUBLIC ACCESS/PRIVACY CONCERNS IN THE COURT RECORDS CONTEXT

Another wrinkle complicating the debate about public access versus privacy in the provision of Internet access to court records

156. In fact, the most useful “Sunshine laws” are those that void agreements among private parties to keep facts relevant to maintaining public safety confidential. See Spainhour, supra note 143. As noted above, existing requirements of a showing of “good cause” before issuing protective or sealing orders (together with judicial education) may be sufficient to protect against the kinds of abuses seen in the Bridgestone/Firestone tire and priest abuse cases. See Miller, supra note 134, at 474-77, 490-501.

157. Indeed, George Carpinello discusses the operation of the “good cause” requirement in the context of electronic access to court records, indicating that judicial discretion within articulated bounds can best balance the tension between access and privacy. See Carpinello, supra note 148.
involves the role of the private sector as both a facilitator of access and a consumer, compiler, and aggregator of the data contained in those records. Intense private sector interest in personal information highlights the increasing importance of such information as a commodity. Indeed, some commentators have noted how technology is “commodifying” personal information and have explored the treatment of personal information as “property.” The broad concern about the role private sector information brokers play in threatening individual privacy impacts Internet court records policy in several ways.

First, some court systems turn to the private sector for expertise in establishing systems for providing online access to court case records. This can raise questions about the ownership and use of the Internet access architecture (and indeed the records themselves). Second, some courts provide access to bulk information and aggregated data to private sector entities for background checks or other purposes. Often courts charge fees for this information, raising revenue to support court technology or the general fund. However, the sale of bulk information for revenue enhancement can appear to detract from the courts’ obligation to provide free and open access to records and to remain free from private sector influence in this endeavor. Finally, private sector interest in court records data may influence legislators and lobbyists to push courts to implement access architecture and policies that tend to serve private commercial interests more than the public interest in access, transparency, and appropriate security and privacy protections. As one commentator notes:

[only in the for-profit private sector are there the resources both to produce sophisticated information and to purchase the finished product on a commercially viable scale. Public sector information services were once fairly widely available on a free or low-cost basis, but in this era, market principles


The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information. Moreover, a strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data.

Id.
of user-pay, cost recovery, and servicing "clients" have led to the virtual privatization of public-sector information. Even those once-privileged bastions of state information secrecy, the security and intelligence agencies, are flogging their information services to the highest bidders in the private sector. Governments increasingly post free information on the Internet, but this is mainly for democratic legitimation of their cost-recovery supply to the private sector: the very fact that information is freely available is generally proof of its relatively low value as a commodity.\footnote{Whitaker, supra note 112, at 71.}

The argument that public information is being subjected to virtual privatization to become useful may be made with respect to court records. Private vendors have demonstrated intense interest in court records and indeed providers of computerized legal research like Lexis/Nexis and Westlaw have a keen interest in providing access to (and cornering the market for) court records information that may be organized and aggregated for useful applications that lawyers and others will purchase.\footnote{See Melissa Barr, Democracy in the Dark: Public Access Restrictions from Westlaw and LexisNexis, 11 SEARCHER 1 (January 2003), http://www.infotoday.com/searcher/jan03/barr.shtml (arguing that LexisNexis and Westlaw are cornering the market for legal research and court record information, some of which previously had been available free of charge). In a time line summarizing 30 years of LexisNexis activity, it is noted that in 2001, LexisNexis acquired CourtLink Corp., the leading provider of web based services to electronically file legal documents and access and monitor court records. LexisNexis, The LexisNexis Timeline: Celebrating Innovation... and 30 Years of Online Legal Research, 13, http://www.lexisnexis.com/presscenter/timeline/30th_timeline_fulltxt.pdf.}

This exacerbates concerns about the government's collection of vast amounts of personal information in secret and explains some of the suspicion about an offer by the government to use the Internet to provide greater transparency regarding its records and functions. Yet much of the reaction to proposals to provide Internet access (and thus greater transparency with respect to this aspect of government) has centered around the concern that despite arguments about greater transparency, the placement of court records on the Internet will only serve to feed the panopticon. That is, that while only minimally enhancing public understanding and oversight of court functions, Internet access will do much more to facilitate both the government's and the private sector's roles as participants in the collection, distribution, and use of individual private information. The
Internet has accelerated a shift in the power of the panopticon from centralized government actors to both centralized and decentralized private actors. Rather than the familiar model of a single governmental Big Brother, individuals now face Big Brother, Bigger Brother (global corporations), and a vast array of Little Brothers and Sisters and Strangers all unseen, watching and waiting to use the information accumulated and aggregated for both positive and nefarious purposes. These observers argue that government action which contributes to the accumulation and aggregation of individual private or sensitive information only makes a bad problem worse.

This sinister view of the power and perils of the Internet pervades much scholarly and popular discourse and has had a profound impact on the debate about finding the appropriate balance between transparency and the protection of individual private or sensitive information. Couple this with the notion of ceding information control to the private sector, or worse, the secret agglomeration of public and private information, and many red flags go up.

In the court records context, online access is developing in a number of ways: some entirely managed by court systems, others handed over to private entities, and still others operating using a combination of the two. In the federal government and in many states, court systems use their own internal systems to provide access to court dockets and information. Private vendors have shown much interest in obtaining court record information to repackage and sell to clients in various forms and for various reasons. Indeed, private sector vendors have been actively

---

161. See generally ROBERT O’HARROW, JR., NO PLACE TO HIDE: BEHIND THE SCENES OF OUR EMERGING SURVEILLANCE SOCIETY, (2005) (describing how increased surveillance capability, computer technology, and the merging of public and private personal data collection have resulted in the collection of vast amounts of personal information that can be used to track, assess, and predict our behavior).

162. See, e.g., Solove, Access and Aggregation, supra note 27; Lin supra note 66.

163. See O’HARROW, supra note 161; Whitaker, supra note 112.


165. The federal courts have developed a cost-based PACER system modeled on commercial computer access systems but belonging to the federal courts. The PACER system requires registration and payment for downloading information beyond a certain minimum number of pages.
lobbying many state governments to get in on the action in online court records. The inclusion of private vendors in the provision of online public court records may lead to anomalous situations such as the possibility that a private vendor establishes an electronic court records system and then goes out of business, leaving open a number of questions about the ownership of the system and of the information contained therein.

Certainly, private vendors’ interest in the information contained in court records highlights its market value and the commercial interest in the collection, aggregation and use of this data for a range of purposes including background checks and consumer profiles as well as the secondary packaging and sale of case searches and court information to lawyers and other interested persons. But once again, because court records are public documents many argue the primary concern should not be in the provision of wider (or “jazzier”) public access by private vendors but rather should be focused on providing effective access and avoiding circumstances under which private vendors might seek to “privatize” and restrict access to public information.

If the information that courts have to sell is commercially valuable, does the free provision of this information, which is used most often to further commercial and “entertainment” (as opposed to public education and oversight) purposes, by placing records online for free, subsidize a growing market in the sale of private parties’ information with no remuneration for the parties? As the number of issues around Internet access to information in general proliferates, it is important that court systems remain focused on the goals and purposes for which courts provide public access to the public documents they produce and that courts develop policies that are consistent with those purposes. Although court systems must be cognizant of the ways in which court record information may be used and misused, there should also be some recognition that ancillary misuse of court records

information should not lead courts to refrain from providing appropriate access that is consistent with the role and purposes of the courts. Nor should courts permit the methods of and policies for providing online access to court records to be driven by private sector interests or pressures.

IV. RECOMMENDATIONS FOR DEVELOPING POLICIES THAT BALANCE THE TENSION BETWEEN PUBLIC ACCESS AND PRIVACY IN THE COURT RECORDS CONTEXT

The tension between providing public access to public documents, including court records, and competing interests such as privacy, security, trade secrets, and government interests in efficiency and fairness, has been around for a long time. Why then, has the access/privacy debate become so thorny for courts in the context of Internet access to court records?

Courts—including judges, court administrators, and court staff—do not operate in a vacuum. Concerns about Internet privacy and security do not go unnoticed by judges and court administrators. Indeed, the toughest questions about privacy and security are often resolved in the courtroom. Thus, when engaged in policy development that seeks to strike the appropriate balance between public access and issues of privacy, security, and effective administration, there can be an impulse to address broader privacy problems like identity theft, stalking, and other misuses of online information. 167 Although there is no doubt that courts should take steps to prevent injury to litigants and to reduce the chances that publicly available information about them will not be misused, it is not the courts’ job to foreclose improved access to public information or to solve broader Internet privacy and security problems. The best way to address broader concerns like identity theft is through effective legislation and

---

167. See, e.g., testimony of Ken Dreifach, supra note 9 (detailing concerns about exacerbating identity theft through online court records access). In my own experience working with New York State’s Commission on Public Access to Court Records, I remember that my initial approach to the project was from a privacy protective perspective that came not only from my own concerns about Internet privacy, but from my prior work with the New York State Attorney General on Internet and consumer privacy protection. As I focused more closely on the role of the courts and on the purposes and importance of public access to court records, I began to see the importance of a more narrowly tailored court records policy that responds to privacy concerns without trying to resolve them and without restricting appropriate access.
serious, consistent, and effective law enforcement. This does not mean, however, that the courts should completely ignore the issues raised by Internet access or refrain from developing or modifying relevant policies.

Rather, courts must confront the policy challenges introduced by Internet access and, consistent with their role and cognizant of the purposes of public access, draft policies that hone existing methods for balancing the public access/privacy, minimize the inclusion of high risk data not essential to court procedures, provide education about the impact of Internet access and, to the extent feasible, address the concerns of various stakeholders. Next, the article will briefly discuss each of these recommendations below.

A. COURTS MUST CONFRONT THE POLICY CHALLENGE RAISED BY THE PROSPECT OF INTERNET ACCESS TO COURT RECORDS WITH A COHERENT POLICY THAT DRAWS ON EXISTING FRAMEWORKS AND THE EXPERIENCES OF OTHER COURTS IN STRIKING THE PUBLIC ACCESS/PRIVACY BALANCE

Contrary to the view of proponents of total unfettered access to court records, there is a necessary and meaningful role for court policymakers in balancing public access with privacy, security, and effective court administration. While court policies are incapable of solving broader problems wrought by the Internet, and should not try to do so. Courts can and should, however, review and modify their policies to ensure that information included in court records, by request, habit, or requirement, is protected from needless risks.168 Ideally, given the ease with which private entities may scan and publish over the Internet paper records, this review should address paper as well as electronic records. Even those courts that decide not to place case records on the Internet but to limit online access to

168. One recommended approach is that courts review the information that is routinely requested of litigants to ensure that it is necessary. For example, Florida's Committee on Privacy and Court Records stated in a recent draft reported that:

The Committee has concluded that Florida court files commonly contain information which is not required by law or rule and which is not needed by the court for purposes adjudication or case management. . . . The Committee makes a series of recommendations intended to substantially minimize the inclusion of such extraneous personal information in court records.

docket information should consider reviewing and revising privacy/security policies regarding information in paper records. Many private companies already provide easy access to case records and may begin placing records online if courts decline to do so. Therefore, whether court systems systematically place court records online or not, courts should be cognizant of the potential for broad public access to all public case records and should implement appropriate guidelines regarding "public" and "non-public" information in all court records.

For example, court policymakers should encourage attorneys, litigants, and judges to consider the circumstances under which sensitive information is really necessary to resolve a case. Such information may range from Social Security Numbers, to detailed medical information, to sensitive personal information in family law cases involving children. A quick scan of a sample of records routinely filed in New York State court revealed that court forms may request data items such as social security numbers and dates of birth in cases in which that information may not be used and is thus unnecessary.\(^{169}\) Similarly, judges should be wary of litigants who include sensitive personal information or even egregious allegations in court documents as a mechanism to "shame" their opponents or gain a litigation advantage.\(^{170}\)

The most difficult task that court policymakers face is how best to identify and address matters that should be dealt with systemically from the kinds of issues that are best resolved on a case-by-case basis. Because of the array of circumstances under which sensitive information may appear in court records, in many instances judges will have to resolve the tensions between access and privacy on a case by case basis. A case by case approach is the only way to ensure that access decisions are to be neither

\(^{169}\) For example, a research assistant searching New York paper court records in a Bronx courthouse easily obtained copies of a death certificate containing details including the date of birth, Social Security number, address, marital status, parents' names, as well as a copy of an authorization to disclose a deceased person's medical records, which included name, address, date of birth, date of death, and Social Security number. (Documents on file with the author.) While some of this information may be necessary given the purpose for which the document is prepared, a re-examination of the nature of the "public" information in the document is warranted.

over-inclusive nor under-inclusive. For this purpose, many existing frameworks, like the "good cause" requirement prior to sealing court case files, may operate fairly well.

Courts should establish general policies to guide judges, attorneys, litigants, and administrative personnel as case records go online and should implement a streamlined process for eliminating from public view information that is clearly not in the public interest and that presents risks to litigants, witnesses and others. Given the importance of public access and the identification of high risk data elements for purposes of individual privacy and security discussed above, court policies regarding public access to court records should focus narrowly on redacting or eliminating data elements that pose the greatest risks to individuals and do not serve the public's interest in judicial oversight and accountability.

Some observers argue that the access/privacy tension can be resolved through the use of technology, including the use of computer programs to redact sensitive data elements or to anonymize information so that individual privacy is protected where bulk or aggregated data is disseminated. In addition,

171. The case by case approach is well established, and is applied to resolve access issues in a variety of contexts. For example, the court in United States v. Moussaoui, 65 Fed. Appx. 881, 887-88 (4th Cir. 2003), describes its method for determining the redaction of pleadings in a terrorism case:

Our practice with respect to a pleading by Moussaoui is as follows. [citations omitted] The pleading is initially filed under seal to provide the Government an opportunity to submit proposed redactions. [The motion to redact is placed in the public file, but the proposed redactions are kept under seal]. Intervenors do not contest the adequacy of this procedure, and we decline to alter it. Redaction of Moussaoui's pleadings is necessary to omit irrelevant and inflammatory material and to prevent Moussaoui from attempting to communicate certain information to others [citations omitted]. The interest of the public in the flow of information is protected by our exercising independent judgment concerning redactions.

Id.; see also Securities and Exchange Commission v. TheStreet.com, 273 F.3d 222, 231 (2d Cir. 2001) ("With respect to all judicial documents, however, we held that, 'it is proper for a district court after weighing competing interests, to edit and redact a judicial document in order to allow access to appropriate portions of the document . . .' ").

172. See, e.g., Carpinello, supra note 148, at 1123.


The same technology that heralds unprecedented public access at minimum cost and maximum ease also enables an automated intelligence that is capable of understanding and processing data in sophisticated and nuanced ways . . . . This technology – Extensible Markup Language (XML) and its family of related
there are those who argue that concerns about the harvesting and aggregation of online information can be minimized through technology that can make case records available one at a time but not in the aggregate and that requires a form of "prove-you-are-human log-in procedure" to prevent automated harvesting of information. 174

While technology may help, the tougher work for courts is in developing policies to ensure the most effective use of technology to achieve the appropriate balance between access, privacy, and security. As one commentator notes:

The policy challenge is to determine the rules and procedures governing the [privacy] divide, and the technical challenge is to build in technical features to execute or enforce those rules and to manage accountability. The overall architecture must include organizational, procedural, and technical features in a framework that integrates these control requirements within business process needs. 176

To meet this challenge, courts should obtain input from a range of court users while keeping in mind the particular role of the courts both generally and with respect to the provision of records access.

browsers, parsers, processors, and standards – permits information in court records to be shared with the public at the courthouse and over the Internet while respecting the legitimate privacy interests of litigants and others who come before our courts.


175. Taipale, supra note 173, at 192.
B. IT IS IMPERATIVE THAT COURTS INCLUDE STAKEHOLDERS IN THE POLICY DEVELOPMENT PROCESS AND LEARN FROM THE EXPERIENCE OF OTHER COURT SYSTEMS

The experience thus far with court access policies on the federal and state levels has shown that an essential step in developing court policies regarding Internet access (and public access generally) is to involve stakeholders including attorneys, litigants, judges, advocates, representatives of various constituencies, and the general public. For most court systems, this policy development has not been easy. The Maryland court system went through two rounds of policy development (including significant public input) before issuing policy guidelines addressing online case record access. The Florida courts have gone through an involved policy development process that began with some clerks placing court records online wholesale, which was followed by a complete moratorium on Internet access to court records. A number of state court systems have spent several years considering, developing, piloting, and implementing court records access policies. On the federal level and in many

176. Indeed, the drafters of the CCJ/COSCA Model Guidelines on Public Access to Court Records stressed the importance of broad public outreach and the inclusion of various points of view in developing court records access policies, noting its importance as part of their own policy making process:
Our “process” was involved but necessary in order to produce the intricate CCJ/COSCA Guidelines product. Inviting, welcoming, incorporating, and facilitating continued participation from a range of individuals and perspectives, using similar mechanisms may be our primary recommendation to states and jurisdictions that wish to use these CCJ/COSCA Guidelines as a starting point for their own deliberations. Include a range of opinions. Facilitate the discussion. Work to obtain a compromise and acknowledge with respect those areas where compromise just is not possible. The resulting product will be richer, and the professional relationships that are built will be essential in implementing rules and routines to both ensure privacy and promote access to state court records.

Steketee & Carlson, supra note 135.


179. See Steketee & Carlson, supra note 135.
states, court policymakers established a fairly involved process for public input prior to drafting Internet access policies. The public process played an important role in educating both the public and the courts about the possible implications of placing court case records online. For example, courts received testimony regarding the potential detrimental effect of Internet access to court records in the contexts of identity theft, domestic violence cases, employment relationships, matrimonial and family law cases, and general snooping on individuals.

The myriad general concerns raised about the Internet have made it difficult to identify optimal policy solutions for balancing access and privacy in court records. This difficulty stems less from the particular issues raised in the court records context and more from generalized Internet concerns like identity theft, stalking, and the worldwide airing of matters considered personal and private. When court policymakers try to grapple directly with these broader issues, their goals can become diffuse and appropriate solutions may seem unattainable. As the policy process in many state courts demonstrates, it takes much discussion over time for policymakers to identify and clarify the boundaries between broader Internet concerns and the more particularized issues that should drive court records access policies. It is not hard to imagine why. Over the last few months, for example, there have been several reports of unprecedented breaches of online security resulting in the release of sensitive information, such as Social Security and account numbers of many thousands of individuals which raises the

---

180. See, e.g., Steketee & Carlson, supra note 135; Deyling, supra note 147, at 1.
181. Courts also received testimony about the benefits of online access to court records for media access, background checks, and public education about the courts. See, e.g., COMMISSION ON PUBLIC ACCESS TO COURT RECORDS, REPORT TO THE CHIEF JUDGE OF THE STATE OF NEW YORK, supra note 3, at Exhibit 3.
182. For example, the recent report of the Florida Committee on Privacy and Court Records explicitly recognized the difficulty Committee members had in reaching consensus:

The breadth and complexity of the subject under study is such that intelligent, reasonable people can and do reach different conclusions about law and policy. Indeed, public input to the Committee includes passionate, articulate arguments on a number of sub-issues. It should therefore not be surprising that the Committee could not reach consensus on several major issues, indeed it would be remarkable if it did.

Jon Mills, Chair, Committee on Privacy and Court Records, Supreme Court of Florida, Final Report of the Committee on Privacy and Court Records (August 16, 2005) at 4.
specter of mass identity theft. The concern that making court records available online will exacerbate these problems and possibly do so with an apparent government stamp of approval resonates with many court policymakers. Current legislative proposals make reference to public records and the interplay between government and private data collectors as issues to be considered when seeking to protect individuals from the misuse of their personal data.

In addition, the issues and questions raised in connection with Internet access to court records (and in the context of the “secret settlement” debate) warrant a re-assessment of current access policies in both real space and cyberspace. The deluge of concerns unearthed during public hearings and public comment periods gave many court policy makers pause.

183. See recent reports of data theft of records of ChoicePoint, LexisNexis and others, supra notes 18-28 and accompanying text.


185. One aspect of the Internet access policy debate on both the federal and state levels involves whether paper and electronic versions of court records should be treated differently (generally with greater redaction of electronic records) or whether the only distinction should be between public and nonpublic information regardless of the record’s form. The general consensus appears to be that a “public is public” court records policy makes most sense. This, in turn, supports a general reconsideration of the data elements requested and permitted in public court records. See Steketee & Carlson, supra note 135, at 22. “These CCJ/COSCA Guidelines apply to all court records regardless of the physical form of the court record, the method of recording the information in the court record or the method of storage of the information in the court record.” Id.

186. Policy development in this area has tended to be relatively slow and deliberate, due in part to the range of concerns raised by stakeholders and in part to institutional limitations that range from technological expertise to staffing concerns. See, e.g., PRELIMINARY RECOMMENDATIONS OF THE MINN. SUP. CT. ADVISORY COMM. ON RULES OF PUB. ACCESS TO RECORDS OF THE JUDICIARY, REP. FOR PUB. COMMENT, IN RE: SUP. CT. ADVISORY COMM. ON RULES OF PUB. ACCESS TO RECORDS OF THE JUD. BRANCH, 9-10 (January 21, 2004). The Report stated:

The advisory committee's preliminary recommendation on Internet access should be viewed as the first step in a go-slow approach to providing more remote access to information. As indicated above, courts that have simply begun posting all public records on the Internet have encountered numerous problems and have had to pull back and reconsider their policy in light of privacy concerns raised by persons identified in the records. The committee agreed that the potential for damage to individuals necessitates a careful approach.

Id.
As more and more court systems are realizing, the answer to the complex questions raised by Internet access is not to refrain from placing court records online. Nor is it to avoid the development of policies addressing public access to court records by allowing policy to develop by default. Court policymakers must recognize that the focus of any across-the-board policy is necessarily limited given the courts’ obligation to provide access and the fact that many of the problems articulated regarding Internet access are beyond the scope of the courts’ role.

C. COURT RECORDS ACCESS POLICIES MUST RESPECT THE UNIQUE ROLE OF THE COURTS IN OUR SYSTEM OF SEPARATED POWERS AND CHECKS AND BALANCES

Courts and judges must craft policies that are consistent with the judiciary’s role in our tripartite system of separated powers and checks and balances.¹⁸⁷ Judges and court administrators must be clear about the purposes and boundaries

¹⁸⁷. As the Ninth Circuit stated in Spurlock v. FBI, regarding the parameters of a federal court’s authority to make determinations regarding access to records:


Spurlock, 69 F.3d 1010, 1016 (9th Cir. 1995). Although there is some clear delineation of the respective powers of the judiciary, the legislature, and the executive, there is also a great deal of interdependence and overlap among the three branches of government. For example, as the court noted in Stillman v. Dept. of Defense:

In Nixon II, the Court rejected the government’s argument for “three airtight departments” of government as “archaic.” 433 U.S. at 441-44, 97 S.Ct. 2777. The Court has instead consistently embraced the view articulated by Justice Jackson in Youngstown Sheet & Tube Co. v. Sawyer: While the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government. It enjoins upon its branches separateness but interdependence, autonomy but reciprocity. 343 U.S. at 635, 72 S.Ct. 863 (Jackson, J., concurring). In Mistretta, the Court explained, the Constitution “imposes upon the Branches a degree of overlapping responsibility, a duty of interdependence as well as independence the absence of which ‘would preclude the establishment of a Nation capable of governing itself effectively.’ “ 488 U.S. at 381, 109 S.Ct. 647. Indeed, separation of powers principles do not mean that the branches of government “ought to have no partial agency in, or no control over the acts of each other.”

of their policy work. As courts develop policies to address Internet access to court records, it is important that they keep specific focus on the role of the courts versus other branches. To the extent that broader problems related to the Internet's effect on privacy and security affect court administration, court leaders should resist the urge to address them through court policies and should instead encourage lawmakers and law enforcement officials to address them. To the extent that the current legal patchwork of privacy protections is not well equipped to address the reality of the Internet's capacity for intrusion into an individual's private realm and such intrusion affects court functions, court leaders should alert legislators to the particular concerns that arise in the court records context. But again, this does not mean that courts need not develop and implement their own policies to address these concerns within an appropriate framework.

D. COURT RECORDS ACCESS POLICIES SHOULD BEGIN WITH EXISTING COURT RECORD CLOSURE RULES AND CONSIDER WHETHER THOSE RULES SUFFICE OR SHOULD BE ADAPTED OR AMENDED IN LIGHT OF INTERNET ACCESS

The judicial branch, while remaining focused on its role as distinct from the roles of the other branches in addressing tensions among privacy, access, and security in the Internet context, should draw upon existing rules and the well-developed experience of balancing access and privacy tensions in other contexts. The goal with respect to court records is to provide broad access to relevant information at little or no cost to the public. This means access to information that is appropriate for public information, education, and oversight purposes. At the same time, courts must remain cognizant of individual privacy and safety concerns in cyberspace. Courts must have concerns about government transparency and public access to quintessentially public information as well as concerns about court management and the effective administration of justice. To a great extent, these are the same concerns that courts deal with every day under rules regarding requests to seal records or to close courtrooms; they are the same concerns that come up with protective order and FOIL requests. The approaches taken and

188. This is not to say that these issues, even in the context of existing frameworks, are easily resolved. For example, while court records are generally exempt from their state's freedom of information laws, in some states those laws still implicate
the tools used to resolve these tensions should not be forgotten or abandoned simply because the method of access is the Internet. As noted above, there exist, on the federal level and in many states, rules regarding protective orders or requests to seal court documents that may suffice to keep matter that should not be made public out of court records, while requiring a sufficient showing to avoid wholesale closure of records that should remain open. Before imposing new rules or policies, judges and court policymakers should satisfy themselves that existing frameworks cannot effectively address the task. 189

how courts balance records access against competing concerns, often with complicated results. As noted in a November 1, 2004 Memorandum to Florida’s Committee on Privacy & Court Records from the Media and Communications Law Committee of the Florida Bar, “[o]ne issue that has arisen is whether the hundreds of exemptions to Florida’s Public Records Act also apply to court records, after the Buenano decision” (Buenano, in dictum, raised the possibility that the exemptions to disclosure in Florida’s public records act might apply to court records). Memorandum from the Media & Communications Law Comm. Of the Fla. Bar to the Fla. Comm. On Privacy & Ct. Records (Nov. 1, 2004) (on file with author). Noting that the “Florida Supreme Court has repeatedly stressed that access to adjudicatory records of the judicial branch is not governed by [the public records act] because the latter applies only to records of the state’s agencies and does not include the judicial branch,” the memo goes on to say that “a mechanism exists to protect records, or portions of records, when concerns arise. Id. Parties can request closure of court documents when a compelling interest exists in a given case.” Id. In the memorandum, the Media and Communications Law Committee also notes practical problems with automatically applying public records act exemptions to court records: “Applying each exemption... to court records would create an administrative quagmire and be virtually impossible to administer.... Certainly, clerks cannot be responsible for culling through all the hundreds of weekly court filings per circuit for the possible application of about 700 exemptions to each document.” Id. The Florida discussion provides just one example of the many difficulties court administrators face in applying existing policies and frameworks to the prospect of Internet access to court records, in addition to considering the development of new policies.

189. Current proposed E-Government Act amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure take this approach. The proposed amendments begin with existing rules for filing and sealing of court records and provide for the redaction of social security numbers (to the last four digits), the names of minors (to initials), birth dates (to year of birth), and financial account numbers (to the last four digits), while providing flexibility for courts to address particular or novel issues that may arise in the context of public access versus privacy/security. As noted in the introductory statement for E-Government Rules to be released for public comment:

These rules are intended to implement the requirements of the E-Government Act and also the established Judicial Conference policy concerning privacy protection for court filings. But no rule can adequately foresee developments in technology and rights of access to information, especially given the difficult policy choices that have to be made among 1) protection of privacy interests, 2) individual rights to notice and opportunity to be heard, and 3) public access to court filing. This rule only intends to provide flexibility. It necessarily relies on the responsibility of courts to determine, on a case-by-case basis, whether to
Courts also should draw upon experience thus far with different methods for addressing Internet concerns. For example, the most effective legislative approaches to protecting Internet privacy have been those that affirmatively place information about data uses and abuses in the hands of data subjects. Unlike ECPA and other laws and regulations focused on particular forms of data transfer, laws that require notification to data subjects more effectively address Internet privacy and security concerns. Experience has also shown that more legislation is not necessarily better. Consider the many laws currently on the books that have failed to address the most serious concerns about Internet privacy and security. Similarly, in the court records context, enacting more rules or providing less access may not best achieve the goal of balancing access and privacy. Before proposing new rules, courts should examine existing balancing frameworks and consider whether, either in their current form or with amendments, those frameworks can serve to address the Internet access/privacy tension.

E. COURT RECORDS ACCESS POLICIES SHOULD IDENTIFY AND REMOVE FROM PUBLIC VIEW HIGH RISK DATA ELEMENTS THAT DO NOT SERVE THE PURPOSES OF PUBLIC ACCESS

To the extent that particular classes of data are deemed not relevant for public purposes or are found to pose too great a risk to safety or security, a policy decision to exclude those elements wholesale may be appropriate. A policy approach that targets only the highest risk data elements for exclusion from court documents while maintaining the existing discretionary balancing scheme that allows judges to determine more complex cases is reasonable and appropriate. This approach allows courts to target information implicating widespread and high risk privacy concerns (like the dissemination of Social Security numbers) and also to address, case-by-case, more particularized issues in sensitive cases—maintaining transparency in most

---

dispense with privacy protections or instead to provide greater protection for private information, as the circumstances require.


190. See supra note 102 and accompanying text (discussing California Legislation which requires the notification of data breaches to data subjects and the resulting public notification of the Choice Point, MasterCard and other data breaches).
cases.

For example, the federal courts and New York state courts have opted for a narrow policy that applies equally to paper and electronic records and that identifies a small number of data elements to be excluded from (or shortened in) court case records: Social Security numbers, dates of birth, names of minor children, and financial account numbers. These policies treat paper and electronic records in the same manner and rely to a great extent upon existing statutory or rule-based restrictions on access to certain classes of records, as well as on the court’s inherent power to control access to court records subject to a showing of “good cause.”

Different states have developed policies that vary with respect to both the degree of access provided and the level of detail regarding classes of information that are either


192. See, e.g., REPORT OF THE COMMISSION ON PUBLIC ACCESS TO COURT RECORDS 6 (Md. 2002), http://www.courts.state.md.us/access/finalreport3-02.pdf (noting that “[a]ccess should be the same whether the record is in paper or electronic form”).

193. For example, the report of New York’s Commission on Public Access to Court Records refers to existing exemptions to the presumption of openness:

Section 4 of the Judiciary Law grants the court discretion to exclude the public in certain classes of cases: ‘in all proceedings and trials in cases for divorce, seduction, abortion, rape, assault with intent to commit rape, sodomy, bastardy or filiation, the court may, in its discretion, exclude therefrom all persons who are not directly interested therein, excepting jurors, witnesses, and officers of the court.

Supra note 191, at 19. The report goes on to note that the “right to inspect and copy court records has also been limited by numerous statutes” including sections of the Family Court Act, Domestic Relations Law, and Criminal Procedure Law, and a variety of statutes limited access to court case records to “records in a sex offense case that might identify the victim . . . grand jury minutes . . . probation reports and pre-sentence memoranda . . . records that identify jurors . . . mental health records . . . orders of commitment of mentally ill inmates . . . records of adoption proceedings . . . habeas corpus proceedings for a child detained by a parent . . . certain proceedings . . . concerning venereal disease, and . . . concerning HIV-related information.” REPORT OF THE COMMISSION ON PUBLIC ACCESS TO COURT RECORDS TO THE CHIEF JUSTICE OF THE STATE OF N.Y., supra note 191, at 20-24.

194. “[T]he inherent power of courts to control the records of their own proceedings has long been recognized in New York . . . . [T]his power does not depend on statutory grant but exists independently and ‘inheres in the very constitution of the court’ . . . .” Id. at 19; see also Carpinello, supra note 148, at 1091-93 (discussing the function of New York Rule of Court 216.1, which sets forth a “good cause” requirement prior to a court’s sealing a case record in the context of electronic records).
categorically made public or restricted from public access. Some states have declined to place actual case records online and, at least initially, have decided to provide Internet access to docket information only. For example, the July 26, 2001 Report of the Supreme Judicial Court Web Advisory Board of Massachusetts stated: "As a first phase of dissemination of records on the web, the trial courts should confine themselves to docks. This will serve the function of a bulletin board which announces the existence and status of cases that have been lodged. Access to the actual documents, e.g., complaints, motions, and affidavits, involves a second phase of dissemination." Indiana's policy provides for remote electronic access to "(1) litigant/party indexes to cases filed with the court; (2) listings of new case filings, including the names of the parties; (3) the chronological case summary of cases; (4) calendars or docket of court proceedings, including case numbers and captions, date and time of hearings, and location of hearings; (5) judgments, orders, or decrees." The amended access rule also treats paper and electronic case records equally and specifies several categories of excluded information, including: information excluded by federal law and Indiana statute or other court rule,

(c) Information excluded from public access by specific court order; (d) Social Security Numbers; (e) Addresses, phone numbers, dates of birth and other information which tends to explicitly identify: (i) natural persons who are witnesses or victims (not including defendants) in criminal, domestic violence, stalking, sexual assault, juvenile, or civil protection order proceedings; (ii) places of residence of judicial officers, clerks and other employees of courts and clerks of court. (f) Account numbers of specific assets, liabilities, accounts, credit cards, and personal identification numbers (PINs); (g) All orders of expungement entered in criminal or juvenile proceedings; (h) All personal notes and e-mail, and deliberative material, of judges, jurors, court staff and judicial agencies, and information recorded in personal data


assistants (PDA's) or organizers and personal calendars.197

Thus, even some courts that have not committed to placing the full text of case records online have reconsidered court records access policies given the technological ease with which such records may be made broadly available. Indiana's policy, like many others, sets forth specific items for exclusion from public court case records in addition to those already excluded by law, rule, or specific court order.

Some states, like Florida, which have very strong sunshine laws, enacted legislation providing for online public access to electronic records within a specified time period. The legislation required that clerks of court provide indexes of "official records" online 198 (In Florida, "official records" does not include court case records but includes final judgments.199). Although the law was silent with regard to court records, in 2000 some elected clerks of court began posting court case records online.200 In 2001, Florida's Judicial Management Council took up the issue, noted that the Supreme Court has administrative authority over court records, and recommended that it create a statewide policy.201 Partly in response to public outcry about the release of sensitive information in certain case records posted online, the Florida Supreme Court issued a moratorium on electronic public access to court records pending the development of an access policy.202 In 2002, the Governor signed legislation appointing a study committee on public records and restricting Internet access to records in juvenile, family, and probate cases. Florida's Committee on Privacy and Court Records issued its Final Report in August 2005.203 The Report "contains twenty four recommendations organized into three groups.204 Some of the

199. Id.
200. Id. at 20.
201. Id. at 3-4.
202. Id. at 5; see also Jason Krause, Florida Court Orders Records Offline: Privacy Concerns Prompt Ruling in the Sunshine Law State, 3 No. 1 A.B.A. J.E-REPORT 2 (Jan. 9, 2004).
204. The first group of recommendations is described as "primary recommendations
recommendations received the unanimous support of all members, but many did not.”

Notably, the Florida Committee recommended delaying the placement of court records online until difficult questions about structuring privacy exemptions can be worked out. In the interim, the Committee recommended that docket information, calendars and official court records be authorized to be made available. The Committee recommends a systematic review of legislation, rules, and policies related to confidentiality, privacy, security, and court records access. It also calls for judicial and public education regarding expanded access to information contained in court records. The Report, which contains several dissents, reflects the difficulty many court systems have encountered in reconciling privacy and security concerns about

that the Committee urges be initiated in a short timeframe.” Supra note 23. Here, the Committee “recommends that the Florida Legislature and the national Congress enact meaningful privacy reforms consistent with the First Amendment that effectively protect the informational privacy interests of citizens.” Id. at 46. The Committee further recommends that the Supreme Court reduce the scope of confidentiality under existing court rules to expand public access to court records; that ongoing education and appropriate public notices be provided regarding the consequences of broad public access to court records; that there should be greater coordination and oversight of court records policies; and that interim policy allowing court jurisdictions to make certain court records (such as dockets, official court records, court schedules and calendars, and traffic court records) available electronically while a more detailed court records policy is developed. COMM. ON PRIVACY AND CT. RECORDS, FINAL REPORT OF THE COMMITTEE ON PRIVACY AND COURT RECORDS, supra note 203 at 47-51.

The second group of recommendations “presents a series of recommendations designed to minimize the unnecessary introduction of personal information into court records.” Id. at 44. In this group of recommendations, the Committee calls for a systematic review of court rules and approved forms to reduce or eliminate the inclusion of unnecessary personal information in court records; the development of a policy to exclude the publication of extraneous personal information; and the exclusion of discovery information from court filings except for good cause. Id. at 53-55.

The third group of recommendations “provides a framework for a system of electronic access.” Id. at 45. These recommendations begin with the recognition that electronic access to public court records supports efficiency and accountability goals and recommend a revision of court rules to allow remote electronic access to court records following a review and determination regarding how best to address privacy/security/confidentiality issues and statutory exemptions to public access. Id. at 57-61. The recommendations also call for operational guidelines to assist court users regarding confidential information in court files. Id. at 62. The Committee recommendations place the responsibility for protecting confidential information with filers and court clerks. Id. at 64-66. The Committee finds that the “ultimate authority to protect confidential information in court records belongs to the court.” Id. at 65.
information in court records with the interest in broad public access.

Several courts have issued reports and/or recommendations, or have enacted rules or legislation addressing public access to court records. The federal courts, and state courts in New York, Maryland, California, and other states are moving forward with the placement of full court case records online (though several begin by placing only docket information online). Many have taken a restrained, targeted approach to restricting access to sensitive information.

The list of data elements categorically excluded from case records varies from state to state, depending to some extent on the degree to which case records are being made available and the extent to which a particular state precludes public access to certain categories of cases and information. As noted above, some courts have identified a very limited number of items to be excluded from public access. Others have developed more extensive lists. The CCJ/COSCA Guidelines set forth an extensive list of possible items to be excluded from public access.\(^{205}\) State court policies drafted thus far vary with respect to the precise data elements excluded from public access.

To a great extent, the federal courts, New York, Indiana, and courts in other states that exclude whole classes of sensitive cases like matrimonial, adoption, juvenile, and family law cases from public access, have fewer problems to solve than courts that permit public access to these kinds of cases.\(^{206}\) Some of the

---

205. See Steketee & Carlson, supra note 135, at 45-49.
206. New York law has long provided that many classes of cases are closed to public access, including records in family court proceedings, certain files in matrimonial actions, records sealed pursuant to statute such as criminal cases that terminated in favor of the accused, or involving youthful offenders, among others. REPORT OF THE COMMISSION ON PUBLIC ACCESS TO COURT RECORDS TO THE CHIEF JUSTICE OF THE STATE OF N.Y., supra note 191, at 20-26. The federal courts' jurisdiction generally does not include cases like family and matrimonial in which sensitive personal information is implicated, and federal courts hear fewer cases involving medical issues such as personal injury or malpractice matters. Id. at 25-26. However, concerns were raised about public access to sensitive personal information in bankruptcy cases, which are required by statute to be publicly accessible under 11 U.S.C. §107. Id. at 56-57; see also Office of Justice Programs of the Admin. Office of the U.S. Courts, Privacy and Access to Electronic Case Files in the Federal Courts (1999), http://www.uscourts.gov/privacyn.pdf (recognizing the need to review judiciary policies in the context of new technology). Section 107 has been amended to provide that "[t]he bankruptcy court, for cause, may protect an
thorniest questions surrounding online access involve issues such as domestic violence and stalking, bitter matrimonial disputes, and cases involving children. These are cases that clearly involve sensitive matter but that also call for public oversight. Many of the tensions involved in these kinds of cases can only be addressed through education and experience with the consequences of online access.

F. COURTS SHOULD AFFIRMATIVELY AND AGGRESSIVELY EDUCATE THE BENCH, THE BAR AND THE PUBLIC ABOUT THE IMPLICATIONS OF INTERNET ACCESS TO COURT RECORDS

An important element in reaching the goals of online access to court records while avoiding identified perils is affirmative, appropriate education of judges, court personnel, attorneys, and the public. This is an element which was included in the CCJ/COSCA Model Guidelines on Privacy and Public Access to Court Records but has received relatively little attention thus far in the policy making process (though it has been mentioned by several courts as a component of their court records access policies). Just as legislation requiring companies to inform data subjects about the use (and potential misuse) of their personal information has proven effective in combating identity theft and other misuses of personal information, education can play a critically important role in addressing the concerns raised


207. Steketee & Carlson, supra note 135, at 64-69. Section 8.00 of the Guidelines addresses the “Obligation of the Court to Inform and Educate” and includes reference to providing information to litigants, judges, court personnel, and the public about access to information in court records, and education about the process to change inaccurate information in a court record. Id.


Notice and Education Regarding Personal Information. Attorneys and the general public are not sufficiently aware of the loss of privacy that can occur due to the inclusion of personal information in a court file. The Supreme Court should direct that ongoing education be undertaken and appropriate public notices be provided regarding the loss of privacy and its consequences that can occur due to the unnecessary filing of personal information in court records.

Id. (recommending that “the Supreme Court direct that continuing legal education requirements for attorneys and judges include education on the privacy implications of the inclusion of personal information in court records and the duty to protect the privacy interests of clients”).
in the court records context. Judicial education can help to clarify for judges the circumstances under which restriction of access to records is appropriate as well as circumstances under which closure, even when agreed upon by the parties to litigation, is inappropriate as a matter of public policy. Attorneys can be educated regarding plans for online access to case record information, areas of concern that may call for requests for closure, and the procedures to be followed to seal or redact records. The general public also should be provided information about the potential availability of court records on the Internet for public information purposes, the concerns that might arise for litigants, witnesses and others involved in cases, and the procedures for accessing cases, seeking requests to seal, and correcting errors.

Some state courts are beginning to focus on the role of judicial and public education in achieving the twin goals on public access and individual privacy and safety. For the most part, however, aside from the information that is being disseminated as part of the public hearing process in conjunction with court records access policy development, education remains on the back burner despite its potential to help address some of the difficulties presented by online court records access. Education should be an essential component of court policy work in this area.

CONCLUSION

Much of the policy struggle around Internet access to court records stems from the courts' (largely unspoken) attempt to address and respond to broader concerns about Internet privacy that go well beyond the existence of sensitive information in court records. The answer to these concerns is not to refrain from placing court records online to avoid the policy questions raised. The courts' efforts to provide some measure of control over particularly sensitive information while providing greater access to court records are necessary and appropriate.\(^{209}\)

\(^{209}\) But the necessary legal and policy changes should not begin and end with the courts. The impetus for raising the questions about individual privacy and security in the context of admittedly public court documents stems from broader issues of intrusive, privacy-threatening, and often dangerous information-gathering and aggregation that now include government, corporate, anonymous individual aggregators.

Today's concerns about privacy in public records stem from not only from
The careful approach that many courts are taking in balancing privacy and security concerns with the greater public access promised via the Internet is appropriate. It is also an important component of the overall discourse on Internet privacy and security and government (and corporate) transparency. Court systems should be encouraged to use the Internet to provide greater public access and transparency. In doing so, they should draw upon existing tools for balancing inherent tensions between access and privacy/security. At the same time, courts

traditional notions of government as Big Brother but also from notions of a whole family of data mining and aggregation of vast amounts of personal information from a combination of government and private sources. To the extent that the courts and other government agencies contribute to the private aggregation of personal information, government also must take responsibility for establishing a framework within which individuals can gain control over their information. There is a need to move beyond the patchwork of privacy protections to provide more practical ways for individuals to exercise a measure of control over the treatment of their information.

Post 9/11 there is a greater acceptance among many members of the public that their privacy will be compromised in the interests of national security. The USA Patriot has demonstrates a trend in law enforcement toward diminishing both individual privacy protections AND government transparency. The 9/11 Commission report discusses the fact that information affecting national security is not shared horizontally among government agencies and that this should occur for purposes of identifying possible terror threats. Ironically, the corporate sector has mastered the art of gathering, sharing and aggregating vast amounts of information and sharing that information, for profit, among untold data purchaser seeking to profile and market to each and every one of us.

In this environment, what can possibly be done to protect individual privacy and security and the integrity of the identity that has been formulated from the bits of data collected about each one of us? The answer to that question lies in more effective legislative efforts such as those that require notice to data subjects that their information has been compromised. Such proposals should not occur in a vacuum. Rather, an effort must be made to review and revise privacy protective legislation to ensure both that gaps are filled and that redundancies and ineffective and counter-productive approaches are removed. Indeed, as new legislation is adopted, there should be an effort to take overlapping ineffective or redundant laws off the books.

The problem is that from a political perspective, the money and clout lies with data aggregators rather than data subjects. Perhaps continuous bad press about security breaches and examples of serious harm will be the impetus to force the adoption of legislation that effectively protects individual data subjects. Current incentives in both the private and the government realms favor greater commercial and government access to individual information and less transparency about the collection and use of this information. On the government end, fears about terrorism have rendered people more willing to tolerate ever greater intrusions into personal privacy in tandem with increased government secrecy about the acquisition and use of this information. On the commercial end, the monetary incentives for collecting information for purposes of target marketing, trend tracking, debt collection and other moneymaking purposes far outweigh any existing negative consequences for the misuse of information.
should develop policies and practices that eliminate from public view (and perhaps from court records generally) high risk data elements that are not germane to the public purposes of access, while retaining discretion to safeguard sensitive information within public case records and proceedings.

Consistent with their role in our system of separated powers and checks and balances, courts must keep the focus of their access policies on the courts’ role as administrators of justice and on the reasons for providing public access that are related to that role. To ensure that judges and court personnel do this in a manner that is consistent with the appropriate balancing of competing concerns, efforts should be made to improve judicial education and the education and training of court personnel and lawyers to smooth the transition to the paperless court and to avoid the imposition of blunt and overbroad (or overly narrow or non-existent) restrictions. At the same time, to address the broader privacy and security concerns posed by Internet access, courts should communicate to the legislative branch the concerns they see that relate to court records information and encourage legislation that cabins private sector and government use of personal information so that courts may remain focused on their core interests in public access that promotes transparency, public confidence, and effective judicial administration.