The Public Record:

Information Privacy and Access

A New Framework
for Finding the Balance

Fred H. Cate and Richard J. Varn

Printed in the United States of America

Recommended citation: Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (1999).

Additional copies of ***The Public Record: Information Privacy and Access—A New Framework for Finding the Balance*** are available without charge from the Coalition for Sensible Public Records (CSPRA):

CSPRA
1200 New Hampshire Avenue, NW
Suite 440
Washington, DC 20036
www.cspra.org

The Public Record:

Information Privacy and Access

A New Framework
for Finding the Balance

Fred H. Cate and Richard J. Varn

About the Authors

Fred H. Cate is Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute at the Indiana University School of Law–Bloomington, and Senior Counsel for Information Law in the Indianapolis law firm of Ice Miller Donadio & Ryan.

Richard J. Varn is Chief Information Officer of the State of Iowa, on leave from the University of Northern Iowa, and President of RJV Consulting.

The development and distribution of this paper was funded by the Coalition for Sensible Public Records Access (CSPRA). The members of the Coalition are: Acxiom Corporation, Donnelley Marketing, The Dun & Bradstreet Corporation, Equifax Inc., Experian, First American Real Estate Solutions, Lexis Nexis, The Polk Company, and Trans Union.

The authors alone are responsible for its contents.

Executive Summary

The open public record system has been the mainstay of the U.S. democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports. The American open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want. As the Federal Reserve Board reported to Congress in the context of financial information: "*[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy*."

"Open access to public records is a cornerstone of American democracy. Such access is central to electing and monitoring public officials, evaluating government operations, and protecting against secret government activities. Open access recognizes that citizens have a right to obtain data that their tax dollars have been spent to create or collect."

The public record also raises concerns about information privacy. It is no exaggeration to say that access to and privacy of public records about individuals are virtually always in tension. Recently, however, pressures from European regulators and growing concern over the computerization of data have heightened both the importance and the difficulty of balancing access and information privacy. The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to "profile" individuals, thereby heightening concerns about personal privacy.

The number and complexity of the issues surrounding public records make impossible the implementation of bright-line rules for balancing access and information privacy. Instead, policymakers need a framework to evaluate when and how the law should protect privacy and access interests and how to balance the maintenance of the essential public records infrastructure with legitimate concerns about harms that may result from inappropriate use. Balance is the key.

Decades of legislative, administrative, and judicial experience suggest that the following twelve principles should help guide the process of balancing access and information privacy:

1. **Policymakers Should Identify and Evaluate Conflicting Interests**—Decisions regarding privacy and access inevitably affect and are affected by other important interests. It is therefore essential that any policymaking process identify and examine those interests carefully to determine how they are implicated by a proposed law or regulation and to what extent they can—and should—be accommodated.

2. **Privacy Solutions Must Respond Reasonably to Defined Problems**—Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy.

"More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the 'right to be let alone,' also argued that '[i]f the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects.' He proposed a 'companion piece' to his influential *Harvard Law Review* article, 'The Right to Privacy,' on 'The Duty of Publicity.'"

3. **Limits on Access to Protect Privacy Should be Effective and No More Restrictive Than Necessary**—The accommodation between access and privacy needs to be carefully crafted, so that we continue to permit as much access as possible without unnecessarily invading privacy. In no event should limits be imposed on access to, or use of, public record information to protect privacy if those limits will not in fact be effective in solving identified problems. Moreover, the government should not impose broad limits on access to protect information privacy where effective, extra-legal mechanisms exist that permit a more sensitive and individualized balancing of access and privacy interests.

4. **Privacy Interests are Limited to Personally Identifiable Records**—Access to government records that do not identify individuals should not be restricted on the basis of protecting privacy. Anonymous and pseudonymous records pose no meaningful privacy threat.

5. **Enhancing State Revenue is Not a Privacy Problem**—The government should not use privacy claims as a pretense for raising revenue, enhancing the competitive position of state-published information products, or restricting access to information for other purposes.

6. **Public Information Policy Should Promote Robust Access**—Information policy should facilitate as much access as possible without harming privacy interests.

7. **There Should Be No Secret Public Records**—The public should be able to easily discover the existence and the nature of public records and the existence to which data are

accessible to persons outside of the government. In many cases, it may be desirable and appropriate for the government to inform citizens about who is using their public records and for what purposes. Obviously, access to records is not appropriate in all cases, but this principle recognizes that access serves broad and important purposes.

8. **Not Every Privacy/Access Issue Can be Balanced**—Despite the importance of balancing, it is not appropriate in every case. The courts have established that there are some instances where the societal interest in access is so great that it trumps all privacy concerns. Similarly, the privacy of some types of records is of such importance to our society that it outweighs access interests.

9. **Systems For Accessing Public Records and, Where Appropriate, Controlling Their Use Should Not Be Burdensome**—The mechanisms for accessing the public records and for allowing individuals to protect the privacy of records concerning them should be easily accessible and no more burdensome than necessary.

10. **Information Policy Must Ensure the Security of the Public Record Infrastructure**—The government must ensure that public records are protected from unauthorized access, corruption, and destruction.

11. **Education is Key**—An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions. Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues.

12. **The Process for Balancing Access and Information Privacy Should Be Sound**—Government should have a process for balancing access and information privacy issues that is informed, consistent, and trusted. This process should be in place before one evaluates any new access or privacy issues. The process should draw heavily on expertise and existing data, involve as many of the affected parties as possible, apply these principles faithfully, focus on real and effective solutions, and provide for the automatic termination and/or frequent re-examination of those solutions to ensure their effectiveness and precision in the face of fast-changing technologies.

"What is needed today more than ever is a meaningful way of thinking sensitively and practically about ways of better protecting the privacy interests of citizens, without unnecessarily compromising access to public record information and the broad benefits such access brings. Balance is the key."

Neither information privacy nor access is an absolute. The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible. This is, of course, not always possible. There are times when the society will reject a perceived intrusion that has great benefit and accept a substantial intrusion that has little benefit. The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes.

We must think clearly and precisely about the values served by access and privacy. We must consider the extent to which the public actually and reasonably expects that given information in the public record will be or should be kept private. Finally, we must determine whether targeted and effective protections for privacy can be constructed without denying completely the public's access to information. The cost of doing any less is real, considerable, and will be borne by us all.

"The law has traditionally balanced access and data privacy by providing for disclosure of all information held by the government, except where such disclosure would offend a specific, enumerated privacy interest."

Introduction

The open public record system has been the mainstay of our democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports. Over the past 35 years, however, the increasing computerization and expanding volume of, and ease of access to, public records have raised fears about their misuse. The number and complexity of the issues surrounding public records make impossible the implementation of bright-line rules for balancing access and information privacy. Instead, policymakers need a framework to evaluate when and how the law should protect privacy and access interests and how to balance those interests when they conflict.

"It is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."

—Federal Reserve Board

This paper suggests such a framework for policymaking that balances the maintenance of the essential public records infrastructure with legitimate concerns about harms that may result from inappropriate use. (For possible ways of categorizing public records, see the Public Records Classification Options in Appendix A.) The paper draws on an extensive review of information privacy and access literature, economic and legal research, interviews, and the diverse experience of the co-authors. In the three sections that follow, we discuss (1) the value of public records and why accessibility must be balanced with legitimate privacy concerns, (2) the principles that should guide that balancing process, and (3) the elements of that process itself.

This discussion focuses exclusively on *public* policymaking. Many of the substantive and procedural principles that follow would also apply to policymaking by private organizations; in fact, many businesses and not-for-profit organizations recognize the necessity for balancing access and information privacy interests and reflect that recognition in self-regulatory codes and internal policies. Many private institutions have in place processes, similar to those that we recommend below for government policymakers, for reconciling access and information privacy interests.

Despite these similarities, there are critical distinctions between government and private policymakers: Only the government exercises the constitutional power to compel

disclosure of information and to impose civil and criminal penalties for noncompliance, only the government collects and uses information free from market competition and consumer preferences, and only the government is constitutionally obligated to avoid obstructing information flows and to facilitate the participation of all citizens in democratic self-governance. Therefore, we confine our analysis to balancing access and information privacy issues in the public arena.

Access and Privacy

In 1998 public record information "assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."

—FBI Director Louis Freeh

While the value of information privacy is widely accepted and is the subject of numerous recent articles and books, there has been virtually no attention to the value of an open public record. A balance between demands for privacy and the need for access to public records is impossible to achieve without a better understanding of the important role that accessible public information fills. This section, therefore, discusses the value of the public record infrastructure and the tension between access and data privacy. Later sections address the principles that should guide efforts to resolve that tension and the process for policymaking in this area.

The Essential Infrastructure of Public Records

An essential infrastructure, when effective, is often ignored. We take it for granted. We assume it will work and it disappears from our thoughts. Yet when it is missing or unavailable, only then do we begin to realize how much we depended on it and how it is integrated into many of the things we need and do daily. Anyone who has experienced an extended power outage has had this kind of realization. Similarly, the overarching value of an open records infrastructure is that people and systems assume it will be there and depend on it for a wide variety of activities.

Open access to public records is a cornerstone of American democracy. Such access is central to electing and monitoring public officials, evaluating government operations, and protecting against secret government activities. Open access recognizes that citizens have a right to obtain data that their tax dollars have been spent to create or collect.

The value of this essential infrastructure, however, extends far beyond the government. Its benefits are so numerous and diverse that they impact virtually every facet of American life, to

the extent that we frequently take the benefits for granted. Consider just a few of the essential roles that open public records play:

- Access to public record information provides an important foundation for U.S. capital markets, the most vibrant in the world. The ability to grant credit speedily and appropriately depends on ready access to information about consumers collected in part from the public record. As a result, even major financial decisions are often made in a matter of minutes or hours, instead of weeks or months, as is the case in most other countries.[1] Finally, public records have helped democratize finance in America, meaning that many economic opportunities are based on what you have done and can do instead of who you are and who you know.

- This country's open public record system significantly reduces the cost of credit because the information that credit decisions depend upon, drawn in part from the public record, is assembled routinely and efficiently, rather than being recreated for each credit decision. As a result, American consumers save $100 billion a year because of the efficiency and liquidity that information makes possible.[2]

- Journalists rely on the public record every day to gather information and inform the public about crimes, judicial decisions, legislative proposals, government fraud, waste, and abuse, and countless other issues.

- Law enforcement relies on public record information to prevent, detect, and solve crimes. In 1998 the FBI alone made more than 53,000 inquiries to commercial on-line databases to obtain a wide variety of "public source information." According to Director Louis Freeh, "Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."[3]

- Public record information is used to locate missing family members, heirs to estates, pension fund beneficiaries, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought.[4]

"Commercial users and resellers of public record data improve upon that information by updating it, correcting inaccuracies, and then providing it back to the governmental custodians of the public record."

- Open public records help identify victims of fraud or environmental hazards; save lives by locating owners of recalled automobiles and blood, organ, and bone marrow donors; and protect consumers from unlicensed professionals and sham businesses.

- Businesses rely on public records to choose facility locations, clean up or avoid environmental hazards, schedule the manufacture of consumer durable goods, reduce costly inventory, and prepare economic forecasts.

- Researchers use public information for thousands of studies each year concerning public health, traffic safety, environmental quality, crime, prisons, governance, and a vast array of other subjects.

- Some check verification services use state motor vehicle records to help combat the 1.2 million worthless checks passed every day. One such service used that public record data to verify or warranty $19 billion worth of consumer checks paid to more than 200,000 businesses last year, improving the speed and accuracy of check acceptances, fighting identity theft, and reducing check fraud.

"Reducing access to public information poses specific and grave risks to the U.S. economy and to the provision of services and products that the public values and has come to expect."

- Cable companies and public utilities also use motor vehicle records to verify information about new customers, thereby helping people who have yet to develop credit histories establish new service.

- Our entire system of real property ownership and nearly all real estate transactions have long depended on public records.[5] These records are used to confirm that the property exists, its location, and its defined boundaries. Buyers, lenders, title insurers, and others use these records to verify the title owner. Mortgages, many legal judgments, and other claims against real property cannot be collected without reference to public records.

- Commercial users and resellers of public record data often update them, correct inaccuracies, and then provide the improved version back to the governmental record custodians. They also greatly reduce the volume of inquiries that could otherwise overwhelm a government agency by providing services, Internet sites, and other means to access public records.[6]

- More than two-thirds of U.S. consumers—132 million

adults—take advantage of direct marketing opportunities each year.[7] Public record information helps sellers accurately and efficiently identify consumers likely to be interested in a given product or service.

In sum, the American open public record allows citizens to oversee their government, facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want. As the Federal Reserve Board reported to Congress in the context of financial information: "*[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy*."[8] Yet, it is in the creation of these benefits that many information privacy concerns arise.

The Tension Between Access and Information Privacy

"Privacy" is the subject of many varied definitions and valuations, but it is clear that privacy of information—the interest of individuals in controlling access to and use of data about themselves—serves many essential roles in the growth and development of us as individuals and in our participation in government, commerce, and society. Much of the value of information privacy is abstract. As a result, it is often difficult for political and judicial processes to examine that value, because it varies so greatly according to the individual, the situation, and the benefit received for the privacy lost. Nevertheless, in balancing privacy and access, these intangibles must be considered.

"American consumers save $100 billion a year in mortgage payments because of the efficiency and liquidity that public record information makes possible."

There is also a demonstrable value to data privacy. The free flow of information and the value it represents is dependent in part on privacy policies that engender the necessary level of trust on the part of the citizenry. People must believe that their best interests or those of the society are being promoted by the use of public records. If not, they will avoid or subvert the public records systems whenever possible. Moreover, they may succeed in advocating for restrictive information privacy laws without regard for the value that access provides. It is only in the balancing of privacy and access that we can determine their net value and thereby identify the best policies and processes.

It is no exaggeration to say that access to and privacy of public records about individuals are virtually always in tension. That tension is not new. More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the "right to be let alone," also argued that "[i]f the

broad light of day could be let in upon men's actions, it would purify them as the sun disinfects." He proposed a "companion piece" to his influential *Harvard Law Review* article, "The Right to Privacy," on "The Duty of Publicity."[9] The tension between access and privacy is particularly acute in the United States because of the critical role that both access and information play in our system of government and in our markets. As noted above, the issue is especially important because of the power of the government to compel disclosure of information and the fact that individuals have few alternatives but to comply: The market, which can reflect consumer demand for privacy protection, does not apply to most information processing by the government.

Lawmakers have recognized in cases such as medical records that the important privacy interests of individuals must on occasion temper the constitutional commitment to the free flow of information. Disclosure of some information possessed by the government may reveal intimate details of individuals' private lives without providing any significant public benefit. In such situations, the government appropriately restricts access or requires that identifying details be removed from the information before it is released.

"The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to 'profile' individuals, thereby heightening concerns about personal privacy."

The law has traditionally balanced access and data privacy by providing for disclosure of all information held by the government, except where such disclosure would offend a specific, enumerated privacy interest. This is true of virtually all state and federal public records laws. The federal Freedom of Information Act, for example, requires disclosure of all records other than (1) "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," and (2) records compiled for law enforcement purposes "to the extent that the production of such [information] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[10] Under the FOIA, these records may be withheld if the agency believes that the privacy risk justifies it. The laws of the states and the District of Columbia follow a similar pattern: *disclosure is the rule, privacy is an exception.*

Laws applicable to the private sector reflect a similar balance. The Fair Credit Reporting Act, which for almost three decades has established the regulatory framework according to which consumer information is collected and used in the United States, permits the broadest possible access and use of public record information, subject to specific but vital protections for consumer privacy.[11]

To respond to privacy concerns, many private organizations that use public information offer important privacy protections of their own. For example, the Direct Marketing Association operates the Mail Preference Service and the Telephone Preference Service. With a single request to each, it is possible to be removed from DMA-member company mailing and telephone solicitation lists.[12] Similarly, many of the major companies that provide information on individuals, much of which is drawn from public records, have agreed to abide by Individual Reference Services Group Principles. These principles not only establish privacy protection standards, but also require annual compliance audits by third parties and a commitment not to provide information to entities whose practices are inconsistent with the IRSG Principles.[13]

Today, however, pressures from European regulators and growing concern over the computerization of data have heightened both the importance and the difficulty of balancing access and information privacy. The very technologies, such as the Internet, that expand opportunities for easy, inexpensive access to public records also increase the ability of the government and citizens to search and collect disparate pieces of data to "profile" individuals, thereby heightening concerns about personal privacy. While there are a growing number of concerns related to actual uses and abuses of public records (*e.g.,* identify theft), many privacy concerns are hypothetical or mythical. They reflect fear of the unknown rather than specific harms, or are about privacy in general and only nominally related to public records. Such fears cannot be dismissed out of hand, but care must be taken not to overvalue them in the balancing process.

"The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible."

What is needed today more than ever is a meaningful way of thinking sensitively and practically about ways of better protecting the privacy interests of citizens, without unnecessarily compromising access to public record information and the broad benefits such access brings. Balance is the key.

Principles for Policymaking

What principles should guide the process of balancing public access with information privacy? Decades of legislative, administrative, and judicial experience suggest that the following twelve principles should help guide the process of balancing access and information privacy:

1. Policymakers Should Identify and Evaluate Conflicting Interests

Decisions regarding privacy and access inevitably affect and are affected by other important interests. These interests are often socially valuable and deeply held. It is therefore essential that any policymaking process identify and examine those interests carefully to determine how they are implicated by a proposed law or regulation and to what extent they can—and should—be accommodated.

In addition to the broad concepts of "privacy" and "access," those interests often include, but are not limited to, concerns about:

- Equality—Equal and open access to public records helps level the playing field in such endeavors as issue advocacy, lobbying, and elections. It also gives small and start-up businesses access to some of the same databases as large and established players.

- Freedom—Public records about the functioning of government, private individuals, and companies can be used to keep them in check so they do not impinge on the rights of others.

- Participation—The more people know about their world and about government in particular, the greater the likelihood that they will increase the quantity and quality of their contributions to participatory and representative democracy.

- Security—Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both privacy and access, cause explosive public reactions, and create governmental liability.

- Economic Opportunity—A substantial portion of the current economy is in part dependent on the free flow of public records and limiting their use or availability will have economic consequences. Moreover, public and private records are the raw materials for the emerging economy and for the knowledge revolution of the Information Age.

"Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy."

- Quality of Life—The use of information systems can free people from rote tasks and greatly speed transactions. Getting the amount of privacy one needs, however, also may affect quality of life.

- Intangible Values and Uncertain Fears—A catchall value for things people like and dislike. Often we dress up our likes and dislikes in more eloquent terms, but often decisions and opinions are really based on this simple amalgamation of our feelings.

- Efficiency—Efficient access to public records saves time, resources, and money. Without complete and reliable information, much of the benefit of information technology cannot be realized. However, we can also be so efficient as to impinge on individual freedoms.

- Fairness—Is the process by which a law or rule is nacted, or by which a decision is reached, fair, and is the outcome fair to all of the parties involved?

As this list suggests, identifying and evaluating the interests at stake when balancing privacy and access are not easy tasks, but they are essential if the outcome of the process is to be effective, efficient, in the public's interest, and fair.

"American consumers save $100 billion a year in mortgage payments because of the efficiency and liquidity that public record information makes possible."

2. Privacy Solutions Must Respond Reasonably to Defined Problems

Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy. The Supreme Court has long asked in the context of various constitutional issues, such as Fourth Amendment challenges to government searches and/or seizures: What expectation of privacy is implicated by access and how reasonable is that expectation? When evaluating wiretaps and other seizures of private information, the Court has inquired into whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.[14]

The inquiry regarding the reasonableness of the privacy concern should take into account three specific issues: (1) the sensitivity of the information disclosed; (2) the use to which the information is to be put; and (3) privacy

protection afforded similar information in the past. These inquiries help prospectively arrive at a common-sense value on the privacy side of the access-privacy balance.

Furthermore, the solution should go no further than is necessary to solve the problem: Access should be limited no longer and to no more data than necessary to protect privacy. Laws that purport to stop a harm to privacy but are ineffective harm both privacy and access. Such laws at once constitute an empty promise and a restraint on openness and freedom of information.

3. Limits on Access to Protect Privacy Should be Effective and No More Restrictive Than Necessary

The accommodation between access and privacy needs to be carefully crafted, so that we continue to permit as much access as possible without unnecessarily invading privacy. For example, both access and privacy interests might be served by delaying access to certain law enforcement records until a pending investigation is completed. In other cases, removing (known as "redacting") particularly sensitive information from documents otherwise made public might protect the individual's privacy interests and be preferable to denying access altogether. In no event should limits be imposed on access to, or use of, public record information to protect privacy if those limits will not in fact be effective in solving identified problems.

"While there are a growing number of concerns related to actual uses and abuses of public records, many privacy concerns are hypothetical or mythical . . . . Such fears cannot be dismissed out of hand, but care must be taken not to overvalue them in the balancing process."

Government should not impose broad limits on access to protect information privacy where effective, extra-legal mechanisms exist that permit a more sensitive and individualized balancing of access and privacy interests. The development of privacy seals and certification programs, anonymizing software, user-determined browser privacy settings, prominent privacy policies, industry codes of conduct, and technologies that allow persons to opt out of specified uses of some types of government records are examples of market responses to privacy concerns generally that diminish the need for government action by allowing individuals to protect effectively the privacy of data about them. Clearly, these and similar developments will not eliminate the need for government attention to information privacy, but the number and variety of these initiatives, and the speed with which they are emerging, suggest that they may supplant the need for at least some government actions to protect information privacy.

4. Privacy Interests are Limited to Personally Identifiable Records

   Access to government records that do not identify individuals should not be restricted on the basis of protecting privacy. Anonymous and pseudonymous records pose no meaningful privacy threat. Aggregate data can be used in ways offensive to the privacy concerns of some, but by far these concerns have been best addressed by market-based solutions and private sector codes of conduct. If government action is considered, it should be aimed at the behavior of the offenders and not the records themselves.

5. Enhancing State Revenue is Not a Privacy Problem

   The government should not use privacy claims as a pretense for raising revenue or enhancing the competitive position of state-published information products. This principle does not suggest that the government cannot seek to recoup the marginal or even the operational cost of providing records. But levying excessive charges on citizens to use a public infrastructure that is already paid for with tax dollars is wrong. Moreover, the government should not use claims of protecting privacy as a justification for restricting access to information for other purposes. This principle would seem to many so obvious as to not warrant stating, but many calls for privacy protection today are in fact seeking protection from other harms or are unrelated schemes for generating revenue.

6. Public Information Policy Should Promote Robust Access

   Information policy should facilitate as much access as possible without harming privacy interests. The more robust the flow of data, the more robust the information infrastructure that supports both democratic processes as well as growth of our economy. This reflects the constitutional importance of open public records and the law in most U.S. jurisdictions today: access is presumed unless a specific privacy exemption applies. It also reflects the importance of the public record infrastructure to our polity and our economy. As noted above, it is often possible to target specific privacy harms and leave the public record infrastructure largely intact.

"The development of privacy seals and certification programs, anonymizing software, user-determined browser privacy settings, prominent privacy policies, industry codes of conduct, and technologies that allow persons to opt out of specified uses of some types of government records are examples of market responses to privacy concerns generally that diminish the need for government action by allowing individuals to protect effectively the privacy of data about them."

7. There Should Be No Secret Public Records

An informed citizenry is essential to all checks and balances systems and that includes public record systems. The public should be able to easily discover the existence and the nature of public records and the existence to which data are accessible to persons outside of the government. In many cases, it may be desirable and appropriate for the government to inform citizens about who is using their public records and for what purposes.

Obviously, access to records is not appropriate in all cases (one notable exception in many jurisdictions is investigative files before a criminal case is brought), nor will it always be feasible or advisable to provide information to citizens about the uses made of their records. But this principle recognizes that access not only serves broad social purposes, but also helps build citizen confidence in the public record system, improve the accuracy of public records, helps sharpen citizen understanding of privacy and access implications of the uses of their records so that they may respond appropriately, and contributes to educating all of us about the actual costs and benefits of public record access.

"Information policy should facilitate as much access as possible without harming privacy interests. The more robust the flow of data, the more robust the information infrastructure that supports both democratic processes as well as growth of our economy."

8. Not Every Privacy/Access Issue Can be Balanced

Despite the importance of balancing, it is not appropriate in every case. The courts have established that there are some instances where the societal interest in access is so great that it trumps all privacy concerns. For example, Congress recognized the overriding importance of access, irrespective of the significant privacy interests at stake, when it passed Megan's Law, requiring states to make publicly available the records of convicted child sex offenders for at least ten years after their release from prison.[15] Congress believed that the societal interest in access to the record overwhelmingly outweighed the privacy interests, however great, of the convicted sex offenders. In other cases, information must be public to effectuate the public policy reasons for collecting it in the first place. One example of such a record is bankruptcy filings so that creditors have the opportunity to protect their interests and future creditors can accurately assess risk.

Similarly, the privacy of some types of records is of such importance to our society that it outweighs access interests. Use of certain types of records, such as medical or individual tax records, causes such significant demonstrable

harms that our society rejects that use even when there is a substantial desirable benefit. Productive use of other types of records causes such a visceral reaction that we restrict that use, as demonstrated by the recent outcry over digital driver's license photos. However, one must exercise caution in the application of this principle, as there are many false positives of this kind of reaction caused by sensationalistic journalism and unscientific or biased polling. It is also true that in most cases where a visceral reaction, rather than evidence of specific harms, prompts legislative action, that reaction precedes any understanding of the benefit of the use of the record so no true balancing process was used. Ultimately, policymakers must decide whether the harms are sufficiently clear and severe or the reaction sufficiently genuine and widespread to conclude that it is in the best interests of state or nation to close access to the public record.

9. Systems For Accessing Public Records and, Where Appropriate, Controlling Their Use Should Not Be Burdensome

   The mechanisms for accessing the public records and for allowing individuals to protect the privacy of records concerning them should be easily accessible and no more burdensome than necessary. Information technology systems are emerging that may allow persons to opt out of specified uses of some of their government records. These important systems should not be exempt from the process of balancing the range of interests in the record against the privacy interests of the individual. Moreover, these systems can be costly to run and government must account for this as a spending priority *and* a societal concern. It must balance the cost of such privacy and who benefits against the other priorities of the government, the public, and of those parties directly affected by the loss of access. In using this test it is rarely, if ever, feasible or justifiable to require a person to affirmatively determine the uses of their non-confidential records (known as opting in). This would involve permissions from each of person in the 100 million households in America for each record and/or for each use. The process of responding to countless requests for permission would make the solution worse than the problem.

Drivers' Privacy Protection Act

Federal law currently requires states to restrict access to drivers' information, although this law has been struck down by the U.S. Court of Appeals for the Fourth Circuit on constitutional grounds. Application of this framework calls into question why Congress singled out drivers' information to withdraw from the public record. Motor vehicle registrations reveal little, if any, sensitive information and no more than property tax records, which are presumptively accessible to the public. Moreover, the law was enacted in response to the stalking and murder of actress Rebecca Schaeffer, and its stated purpose was to prevent stalking—an activity already prohibited in most states. And the law permits broad exceptions, including one for private investigators, the very source of the reports used to track down and kill Schaeffer.

10. Information Policy Must Ensure the Security of the Public Record Infrastructure

    The government must ensure that public records are protected from unauthorized access, corruption, and destruction. Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both information privacy and access.

11. Education is Key

    An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions. Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues. The more policymakers and the citizenry know about this issue, the more accurate and satisfying the balancing process will become.

"An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions."

12. The Process for Balancing Access and Information Privacy Should Be Sound

    Government should have a process for balancing access and information privacy issues that is informed, consistent, and trusted by all parties. This process should be in place before one evaluates any new access or privacy issues.

Neither information privacy nor access is an absolute. The goal of policymaking should be to create and apply rational privacy and access policies as efficiently and fairly as possible. This is, of course, not always possible. There are times when the society will reject a perceived intrusion that has great benefit and accept a substantial intrusion that has little benefit. There are those who will fight against the secondary use of a government record and will give the same information away on a warranty card or in exchange for a "free" service or product. The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes.

The Policymaking Process

We have thus far discussed why we should be concerned with balancing access and privacy and what principles should guide that balancing process. Now, we turn to the process itself by which we seek to accommodate privacy and access.

Information policy committees, agencies, and officers that have the benefit of experience and training in this field should exist at each level of government. Moreover, these persons and entities need to be structured to provide the opportunity to balance privacy and access concerns. Where individuals or offices cannot represent both sides of this equation, the policymaking process should be modified to reflect the values of both privacy and access to give the decision-makers the context for striking the balance between them. If, for example, it is considered necessary to have a Privacy Advocate, then there should also be an Access Advocate. Preferably their respective contributions are shared with other neutral experts who seek the proper balance between the two perspectives.

"The government's process for balancing access and information privacy should draw heavily on expertise and existing data, involve as many of the affected parties as possible, apply these principles faithfully, focus on realand effective solutions, provide for the automatic termination and/or frequent re-examination of those solutions to ensure their effectiveness and precision in the face of fast-changing technologies."

Once established, information policy entities can begin to choose their decision-making models to sort through these complicated issues. This should begin with the steps in the process. Each step in this process can determine whether a record is completely public for any uses, public in whole or in part and limited in its uses, or confidential.

A Proactive Policymaking Model

This suggested model, which focuses on proactively balancing the promotion of access and the protection of privacy at the many stages of the decision-making process, begins with specialized information policy officers or entities applying the basics of good public policy. Within the steps described below, these actors will arrange the values on the access and privacy balance. They can then determine the worth of these weights to strike a proper balance. The steps outlined below complete the recommended model in that it brings together the necessary information, the parties in interest, and the desire to make balanced and effective policy in a deliberative process.

1. Gather Existing Data

   Consider what is needed to make sound decisions in this field. If the necessary data do not exist in compiled form, it must be gathered. If a means to gather it does not exist,

those means must be invented. Here is a short, non-exhaustive list of data sources:

- Existing laws and policies in the local jurisdiction, examples of proposed model laws and provisions, and laws and policies from other jurisdictions.

- Existing surveys, opinion polls, and personal knowledge to determine the salient privacy and access issues and the general level of concern. Get a sense as to the percentage of people who are:

  Privacy Purists
  Privacy Pragmatists
  Indifferent
  Access Pragmatists
  Access Advocates

  In this case, being a pragmatist simply means that one's opinion depends on the costs and benefits of each encroachment on privacy or increase in access.

"Most reactions to a notorious occurrence or crisis produce ill-conceived, poorly targeted, and ineffective laws."

- Information policy impact statements because, as noted above, there are often substantial (sometimes unintended) economic effects of public record use. Policymakers should use these impact statements in the same way as fiscal notes, small business and environmental impact statements, and economic multiplier analyses.

- Data, to the extent available, on each of the previously mentioned values relevant to any particular issue under consideration.

2. Educate

   Information policymaking requires multidisciplinary resources. Ideally, academic, government, industry, and public interest groups should work together to create and acquire information privacy and access resources for the policy specialists, the decision-makers, and the public.

3. Identify and Involve the Affected Parties

   In many jurisdictions, privacy advocates, the information industry, and other users of government records are not organized to express their interests, Moreover, many of these entities and associations are naturally myopic in their

interests and cannot be relied upon as a sole source of feedback on policy matters. Consider creating a task force representing industry, government, citizens, and advocates to help sort through and respond to these issues.

4. Use the Principles for Policymaking to Perform the Balancing Process

   With the necessary data and parties at the table, one can now apply the relevant principles to complete the balancing process and decide whether access or privacy interests should prevail or whether both can be accommodated.

5. Choose a Solution

   There are a variety of statutory and market-based solutions to implement a balancing decision.

6. Until This Area Matures, Require Reauthorization of All New Policies

   Unlike mature industries such as transportation, finance, and utilities, the information industry does not have time-tested, high quality economic models or policy creation and review models and processes. The information industry changes so rapidly, in fact, that assumptions and policies can be outdated before policymaking bodies can react. To keep information policies flexible, revisable, and modern it is recommended that sunset and reauthorization clauses be applied to each new access, privacy, and information technology law, policy, or rule.

"Information policy committees, agencies, and officers that have the benefit of experience and training in this field should exist at each level of government."

7. Assess Outcomes

   Policymakers need to assess the effect of their decisions on privacy protection and access concerns to adequately gauge the success of the process.

A Reactive Policymaking Model

There are times when an event or political crisis causes policymakers to react and try to immediately address privacy or access issues. While this is ill advised, the following steps will help guide this type of policymaking process. Most reactions to a notorious occurrence or crisis produce ill-conceived, poorly targeted, and ineffective laws. If possible, delay the policymaking process until the issue can be fully considered.

Information Futures

Information is the raw material for the knowledge revolution of the Information Age. Without complete and reliable information, much of the benefit of information technology cannot be realized. Data warehousing and relational databases, geographic information and visualization systems, and extraordinary technological developments help us better understand our world and behavior of chaotic and complex systems that otherwise defy comprehensive human understanding. In such a technological environment, information is the fuel of our future. The benefits of the Information Age can only be realized if we have the raw materials on which it's essential systems depend: complete and accurate information used within the reasonable expectations of privacy.

However, if political realities will not allow such a waiting period, proceed with the following steps:

1. Determine the Cause of the Privacy Harm or Access Limitation

   What, in short, is really causing the problem? Is it a public record or bad behavior? If it is both, would it be more effective and fair to attack the behavior or place limits on public records?

2. Determine the Direct and Indirect Impact on Persons and Entities

   Despite a perception of a need for swift action, this step is crucial. The information age economy and systems are so interconnected, it is nearly impossible to make a substantial change in one part without affecting many others. It is incumbent on policymakers to find out these effects before enactment. An Information Policy Impact Statement would help force this step in the process and assure that the cure is not worse than the perceived problem.

3. Use the Principles for Policymaking to Perform the Balancing Process

   With as much data and as many of the concerned parties at the table as time will allow, one can now complete the balancing process, deciding whether access or privacy interests should prevail, or whether both can be accommodated.

4. Choose a Solution

   There are a variety of statutory and market-based solutions to implement a balancing decision.

5. Evaluate the Likely Effectiveness

   In the heat of a controversy, it is sometimes politically expedient to just pass a new law to quell the debate, without fully considering its likely effectiveness. While recognizing how difficult it can be to preserve time for thoughtful reflection in the midst of a fast-moving political process, policymakers should strive to evaluate carefully proposed policies to ensure that they will in fact solve the problem, not create unintended problems, and, if such a policy cannot be identified, to wait until an effective

solution can be found and adopted. Ineffective solutions are worse than no solution in the long run, even in politics.

6. Delay Enactment and Require Reauthorization

   To allow time to assess the impact and complete a more thorough policy process, policymakers should require a delay in the effective date and require reauthorization.

Conclusion

The unparalleled openness and accessibility of public records in the United States is not an accident or an historical anomaly. It reflects an understanding that public information is critical for democratic self-governance; that public records belong to the public; and that the widespread availability of public data facilitates opportunity, competition, and prosperity.

"Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues."

Of course, not all information collected by the government is or should be made public. There are important legal protections for confidential financial and health information, trade secrets, and other data which if disclosed publicly would violate a widely shared, objectively reasonable expectation of privacy. This accommodation between information privacy and access is appropriate and necessary in a society that respects the rights of individuals.

Recent efforts to dramatically reduce access to the public record, to close off sources of public information, and to deny the public access to information it has paid to have created or collected threaten the fine-tuned balance between access and privacy. Such a significant shift highlights important issues about the role of the public in the democracy and the right of the public to access its information—information that belongs to the public, not to the government. Equally important, and often ignored in the current debate over the public record, is the understanding that reducing access to public information also poses specific and grave risks to the U.S. economy and to the provision of services and products that the public values and has come to expect.

In terms of policymaking, this area is immature and requires substantial development. Information bears a complex and yet uncharted relationship to the economy and the quality of our lives. Its use and misuse has great potential for good and harm. Great care must be taken in its regulation as each action is likely

to have unintended consequences, positive or negative. Balance, deliberateness, careful review, and caution should form the core of our policymaking efforts.

We must think clearly and precisely about the values served by access and privacy. We must consider the extent to which the public actually and reasonably expects that given information in the public record will be or should be kept private. Finally, we must determine whether targeted and effective protections for privacy can be constructed without denying completely the public's access to information. The cost of doing any less is real, considerable, and will be borne by us all.

"The difficult challenge for policymakers is to pay attention to the concerns of constituents while at the same time seeking to educate them about the costs and benefits and the intended and possible unintended consequences of proposed regulations. This challenge is made all the harder and all the more necessary by the rapid evolution of information technologies and societal attitudes."

Endnotes

[1] The nation's economic boom and the public's standard of living depends in large part on the availability of more than $6.5 trillion in outstanding installment and mortgage credit. Credit reporting agencies and other information compilers collect information on property ownership, outstanding liens and other encumbrances, criminal records, corporate filings, and from hundreds of other public records to maintain the reliable, up-to-date data necessary to support rapid and appropriate credit decisions. Associated Credit Bureaus, Inc., *The U.S. Market at a Glance*, 1998. Although the public record constitutes only one of many sources of credit data, information gathered from public records is often particularly relevant. Public record data includes, for example, information about bankruptcies.

"The open public record system has been the mainstay of the U.S. democracy and economy since the earliest Colonial days. During the last 350 years, this open system has become as essential an infrastructure as roads, telephone lines, and airports."

[2] Diogo Teixeira and Walter F. Kitchenman, "Bureaus Do a Credible Job," *The Banker*, May 1998, at 104. Reliable, centralized, and standardized consumer credit information makes it possible to pool consumer loans and then sell them to investors. As a result, mortgage rates in the United States are estimated to be as much as two full points lower. With outstanding mortgage rates approaching $5 trillion, American consumers save $100 billion a year because of the efficiency and liquidity that information makes possible.

[3] Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 24, 1999. According to Director Freeh the FBI consulted commercial on-line databases to obtain "credit records, real property and tax records; boat, plane, and motor vehicle registration records; business records, including filings with the Securities and Exchange Commission and bankruptcy filings; articles of incorporation; financial information; rental records; news articles; concealed weapons permits; and hunting/fishing licenses" and other "public source information regarding individuals, businesses, and organizations that are subjects of investigations." Access to commercial providers of public record information "allows FBI investigative personnel to perform searches from computer workstations and eliminates the need to perform more time consuming manual searches of federal, state, and local records systems, libraries, and other information sources. Information obtained is used to support all categories of FBI investigations, from terrorism to violent crimes, and from health care fraud to organized crime."

[4] Statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis, before the House Committee on Banking and Financial Services, July 28, 1998.

[5] The U.S. real property system also depends on companies that assemble diverse data from diverse sources around the country, verify its accuracy, and make it readily and affordability accessible to purchasers, sellers, lenders, insurers, and others.

[6] Consumer credit bureaus purchase property tax records in bulk from cities and counties. Those bureaus then respond to more than 600 million requests for credit reports each year. As a result, the cities and counties are relieved of the obligation of responding to those requests individually, thereby dramatically reducing their operating costs. Associated Credit Bureaus, Inc., *The U.S. Market at a Glance*, 1998.

[7] In 1998, direct marketing accounted for $912 billion in sales—12.4% of all consumer sales or an average of $3,378 for every U.S. citizen—and 24.6 million jobs. The $429.8 billion spent on direct mail in 1998 is the largest single contributor to the operation of the U.S. Post Office. Direct Marketing Association, *Economic Impact: U.S. Direct Marketing Today* (4th ed.), 1998.

"While recognizing how difficult it can be to preserve time for thoughtful reflection in the midst of a fast-moving political process, policymakers should strive to evaluate carefully proposed policies to ensure that they will in fact solve the problem, not create unintended problems, and, if such a policy cannot be identified, to wait until an effective solution can be found and adopted. Ineffective solutions are worse than no solution in the long run . . . ."

[8] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (1997) (emphasis added).

[9] Letter from Louis Brandeis to Alice Goldmark (Feb. 26, 1891), in 1 *Letters of Louis D. Brandeis* 100 (Melvin I. Urofsky & David W. Levy eds., 1971); Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193, 193 (1890); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandies, J., dissenting).

[10] 5 U.S.C. §§ 552(b)(6), (b)(7)(C).

[11] 15 U.S.C. §§ 1681-1681t.

[12] Direct Marketing Association, *Name Removal Services* (available at: http://www.the-dma.org/home_pages/consumer/dmasahic.html#removal).

[13] Federal Trade Commission, *Individual Reference Services: A Report to Congress* (1997).

[14] Katz v. United States,389 U.S. 347, 361 (1967) (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).

[15] 42 U.S.C. § 14071(a).

Appendix A

Public Records Classification Options

Public records come in many forms, are collected by many different government agencies, include diverse information, and are used for a wide variety of purposes. In the debate over access and information privacy, there have been many proposals for how to classify public records and the expectations of privacy that may be reasonable for each category. Some of those proposals seeks to classify public records as they exist today; others provide recommendations for how public records might be categorized in the future. Many of those proposals overlap, yet none is entirely comprehensive or satisfactory. However, given the importance of this topic, we include some of the many possible classification options below.

- Unlimited

  Simply put, an "unlimited" public record is one that can be used for any legal purpose. This means any legal government or private primary, secondary, or downstream use and it can be packaged, linked, disseminated, re-disseminated, sold, resold, and reused without limit.

- User-Dependent Limits

  The first distinction in limited use is whether the limit is on governmental or private users. For example private citizens cannot extract data from personal tax records and use other governmental records to analyze it. However, government can do just that. Several states have tax records in data warehouses where data from individual returns and other government and private data is used to determine such things and under-reporting, non-filing, overstating exemptions, and non-payment of student loans while claiming a refund. There are also exceptions for researchers and other special circumstances. Therefore, it is critical to determine if the limited or confidential classification applies to the public, a special private group, or the government.

- Limited Public Records

  Use can be limited to the primary use that is the reason for its collection. If use is allowed beyond the primary use, then the question is whether secondary use (use unrelated to the purpose of collection) is restricted in any way. Finally, if use is allowed beyond secondary use, the question is whether such downstream use (use by third parties after a permissible secondary use) is restricted in any way.

- Transactional Use Only

  Where a record is collected and used only for completing a transaction. Such records may be destroyed after the or transaction is completed. An example would be a credit card number given to get a license. These records are usually kept confidential from the public and have only limited use allowed by the government.

- A Gatekeeper Determines the Use

  A gatekeeper is a trusted public or private official who limits access to public records to protect the subject of the information. A gatekeeper facilitates communications and transactions otherwise impossible if the subject's record is destroyed or made confidential. One way this approach is used is in selected exceptional circumstances to shield a person from an unacceptable harm that would occur if normal procedures and protections were in place. Some examples include witness protection programs, battered spouses, and stalking victims. Another way it can be used is when a non-governmental gatekeeper holds the public records to ensure that they are only used for their proscribed purposes. This is used only where there is extreme concern, fear, paranoia about government misuse or protection of the record. Some examples of this approach that have been used, discussed, or proposed include lists of AIDS victims, gun registration data, and encryption keys.

- An Infomediary Determines the Use

  An "infomediary" is a "a trusted third party, one who connects information supply with information demand and helps determine the value of that information" (http://www.privaseek.com/). Infomediaries would be used where there is a desire to allow for a greater range changeable choices and decisions about how records are used. They could also be used where a person and/or the government want to control the choice process and possibly profit from sale and use of the record.

- Third Party Use Only

  This is where government collects, but does not use the information. Instead, government merely facilitates its use, storage, and transfer. Some examples include bone marrow donor matching programs and medical records in some adoption cases.

- Confidential Records

  Confidential records are those for which there is no public access except for aggregate data in which individual identifiers have been removed. A good example is Medicare records. Government officials or their designees can review them for fraud, waste, and abuse and approve them for payment. However, the only public access to such records is in the aggregate. In other cases, neither the public nor the government is permitted access to a confidential record. An example of this is a sealed court record.