NATIONAL RETAIL FEDERATION

The National Retail Federation's
Protecting Privacy in the New Millennium Series

CONSUMER ACCESS TO PERSONAL INFORMATION

Fred H. Cate

EXECUTIVE SUMMARY

Proposals to require entities that collect or use personal information to provide consumers with access to, and an opportunity to correct, that information often appear sensible at first blush. Closer inquiry, however, reveals that rather than enhancing personal privacy, these proposals seriously threaten it for three broad sets of reasons.

First, they ignore the unprecedented opportunities that U.S. consumers currently have not only to access the information (such as account information) we share in common with the businesses with which we deal, but to do so easily and instantly and to resolve any inaccuracies when necessary. These opportunities reflect business' interest in accurate, up-to-date records, market responses to consumer demands, and existing legal rights. As a result, U.S. consumers enjoy a combination of unprecedented openness, service, convenience, and economic prosperity that is the envy of the world.

Second, many proposals for access to, and opportunities to correct, personal data leave critical issues unresolved and often even unaddressed. The lack of consensus, or even of specificity, is deeply problematic, especially in light of the significant stakes whenever the government undertakes to regulate the collection and use of information.

Third, access and the opportunity to correct personal information always present significant risks for consumers, as well as for businesses. Five of the most common and important of those risks are:

1. *Authentication.* How does an entity required to provide access assure that it is providing access to the right person, especially in light of the fact that all of the measures currently available for authenticating identity require that the individual provide even more personal information about themselves. Mandated access inevitably raises the specter of one individual obtaining access to, or even altering, personal information about another individual. Access then becomes the perfect tool for identity theft, and the government that mandates access the unwitting accomplice of identity thieves.

2. *Greater Data Collection and Centralization.* Mandated access requires businesses to collect, store, and centralize more—not less—personal information. As a result, businesses would be compelled as a matter of law to bring together disparate sets of information—to engage in the very act of "profiling" that privacy advocates abhor—and then to make that new "super" database available via the web and therefore subject to viruses and hackers. These proposals have the effect of greatly increasing the volume, centralization, and vulnerability of personal data.

3. *The Cost of Access.* Few access proposals pay serious attention to the potential cost of providing access and an opportunity to correct personal data. Those costs are measured not only in terms of greater data collection and the potential for wholesale identity theft, but also in very real economic costs, reflected in reduced service and convenience and higher prices paid by consumers and a high volume of litigation over the terms of access and the need for, and adequacy of, corrections.

4. *The Value of Access and Correction.* The fact that mandated access is expensive would pose less of an objection if it were certain to be of sufficient value to warrant the expense, but many proposals would guarantee access even when the access was of no value, and involved information not subject to correction, or information that could not be used to cause any harm to consumers. Is the high cost of access justified if purely for psychological benefit?

5. *The Constitution.* The Constitution says nothing about the privacy of information collected and used by business, but a great deal about the value and protection of information. Guaranteeing a right of access to stored personal information, much less an opportunity to alter that information, interferes as directly with cherished free speech rights as requiring that organizations disclose their membership lists, a requirement that the Supreme Court has repeatedly found unconstitutional.

All of the risks are increased exponentially if access and correction requirements are extended to information collected offline, and increased still further if extended to providing access offline.

Reasonable, targeted access to personal information serves everyone's interests. Proponents of going further—to mandate access that the market does not appear to value and that consumers cannot effectively use—bear a heavy burden of demonstrating both the need and also that the benefits of attempting to meet that need with legislation justify the inevitable risks and costs that such legislation brings.

These proposals for mandated access are not only often ill-formed, leaving unresolved many of the key issues about the cost and benefits of such access, but they also inherently pose significant risks to our privacy, the services and convenience we value, and to our constitutional values.

NATIONAL RETAIL FEDERATION

The National Retail Federation's
Protecting Privacy in the New Millennium Series

CONSUMER ACCESS TO PERSONAL INFORMATION

Fred H. Cate[1]

Congress and a number of state legislatures are considering bills that would require entities that collect or use personal information to provide consumers with access to that information and an opportunity to dispute information that they believe is incomplete or inaccurate. These well-intended proposals often appear sensible at first blush, but closer inquiry reveals that they pose significant risks for consumers, impose considerable costs, and duplicate or even undermine current opportunities for access. Rather than enhance personal privacy, current access proposals seriously threaten it, and should therefore be scrutinized very closely.

The Access Commitment

There is longstanding, widespread agreement in the United States that consumers should have access to the current information that we share in common with the businesses with which we deal. Retailers and other businesses have long provided their customers with access to information about customers' charge accounts, lay-a-way plans, warranty and service plans, and the like. In fact, one of the dominant business trends of the past 50 years has been the steady improvement in the ease and convenience with which consumers can review such information—through 800-numbers, consolidated account statements, automated customer service centers, and, most recently, the Internet. Driven by consumer demand, the extraordinary growth in information technologies, and their own interest in maintaining up-to-the-minute accurate records, businesses have invested heavily in making it easier than ever for customers to obtain and correct account information. Today consumers in the United States have unparalleled access to the information they share with businesses and, increasingly, the chance to not only obtain the information instantly, but also to resolve any inaccuracies.

Few countries share this access commitment. It is not unusual even today in Europe and elsewhere to either have no access to personal information or to have to request access in writing

---

[1]Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington. This paper is published by the National Retail Federation as part of its Protecting Privacy in the New Millennium series. For additional information or to order additional copies, contact the National Retail Federation, Attn: Privacy Project, 325 7th Street, N.W., Suite 1100, Washington, DC 20004, tel (202) 783-7971, fax (202) 737-2849, privacy@nrf.com.

or in person and then wait for weeks or longer to receive the requested information. Despite adoption of a sweeping data protection directive,[2] the access that U.S. consumers take for granted—for example, routine information about the long distance telephone calls we make—is still unavailable or only now becoming available throughout most of Europe.

Current Access Law

Our commitment to access has long been enshrined in U.S. law. For example, both federal and state governments are required by law to provide citizens with access to all of the information they have about them, unless the information fits within one of a narrow list of exemptions (such as if providing access compromises a criminal investigation or national security). This unprecedented degree of access reflects the fact that the government stands in a unique relationship to citizens: Only the government can compel citizens to disclose information and only the government operates wholly outside competitive markets which facilitate the development of privacy protection.

Even private businesses, however, which do not share the government's authority to compel information disclosure or its immunity from market pressures, are nevertheless subject to legal obligations to provide consumers with access to information about them. One of the most important access laws—the Fair Credit Reporting Act—requires consumer reporting agencies (often called credit bureaus) to provide consumers with a copy of their credit report upon request, and to do so without charge if the report was used as a basis of an adverse decision on credit, employment, or insurance.[3]

Similarly, the FCRA implements critical dispute-resolution mechanisms. If a consumer disputes any data, the consumer reporting agency must investigate the claim and delete any disputed data that it cannot verify within 30 days, as well as notify recipients of disputed or inaccurate data of the change. In addition, anyone who *furnishes* data to a credit reporting agency has the legal obligation to correct inaccurate data, notify any agency to which it has reported data, and disclose to any agency to which it is reporting data if those data's accuracy is disputed.

Other laws providing for consumer access to, and the opportunity to correct, personal information include the Family Education Rights and Privacy Act[4] (applicable to financial institutions receiving federal funds) and the Cable Communications Policy Act[5] (applicable to cable operators).

Collectively, these rights, many of which U.S. citizens have enjoyed for decades, are effective both in protecting consumers and in ensuring the accuracy of consumer information

---

[2] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281).

[3] 15 U.S.C. §§ 1681-1681t (1999).

[4] 20 U.S.C. § 1232.

[5] 47 U.S.C. § 551.

because they respond directly to specific situations—the sharing of personal information and the use of personal information to make decisions affecting consumers. These legal obligations do not apply when a business uses its own information (or that of affiliates), information that is not reasonably considered private (such as name and address), information that is proprietary or reveals confidential information either about other consumers or the business, or when information is not used to grant or deny a benefit to a consumer. In short, the close tailoring of these access rights assures that they are available when needed, but that they do not unnecessarily burden either consumers or businesses when they are not.

And it must be remembered that these legal rights, while important, are only one small part of a much broader commitment by U.S. retailers and other companies to ensure that their customers have rapid, reliable access to the information they need—and that they demand—to confidently, comfortably transact their business.

The Push for New Law

Some privacy advocates and even legislators are unaware of, or not satisfied with, the current provision for access, and are proposing sweeping new laws to require more access without regard for either its benefits or costs. All too often, these proposals fail to address, much less resolve, key issues, and they always pose significant risks for consumers.

- **Unresolved Issues**

The Access Process. In the rush to enact access legislation, proponents often ignore the many unresolved issues surrounding access to and the opportunity to correct personal information, even when limited to the online context. For example, what type of access is to be provided—merely an opportunity to review information or should it include the right to correct, amend, challenge, or delete information? How is access to be provided—online, by telephone, via the mail, or in person? When is access to be provided—immediately (in real time), only at specified intervals, upon request, in response to a specific event, annually, or on some other schedule?

The Meaning of "Personal Information." Some of the most difficult unresolved issues concern the personal information to which access must be provided. Information does not come labeled "personal" or "impersonal." Would an access and correction law apply only to information that actually identifies an individual or would it apply to information that *could*, when combined with other data, identify a person, for example, information linked only to a computer address? If the latter, is *any* information excluded? Does the source of the information matter—will access apply to information collected from one person about another? What if the information is observed rather than collected—would the access right, for example, apply to videotapes? What if it is collected from a third party—who must then provide access and to what information? And what about information that is neither observed nor collected, but rather inferred or calculated—must access be provided to information that reflects a retailer's or other business' proprietary conclusions about a customer's likely interests or creditworthiness? Some access proponents even argue that online access and correction rights should extend to

information whether or not it is collected online, thus dramatically increasing the uncertainty surrounding these unresolved issues.

Access Parties. Who must provide access and to whom must access be provided? Consider a simple retail transaction: A consumer uses a bank credit card to buy a gift which is then shipped to the recipient. The retailer collects personal information from the purchaser and about the purchaser when it verifies the credit card, and it may still further observe personal information through its security cameras and other means. Moreover, it records at least the name and address of the gift recipient, as well as what was sent to the recipient. The bank issuing the credit card records the fact that the consumer has made a purchase, where, and for how much. If a debit, rather than credit, card is used, the bank will also access the customer's account, verify the balance, and deduct the amount of the purchase. The shipper obtains the name and address of gift recipient and the value of the shipment.

Who gets access and an opportunity to correct, and from whom do they get it? Must the retailer provide access to the information obtained from the bank about the purchaser? (Recall that if the purchaser successfully attempts to correct some inaccuracy in this information, that information is corrected only in the records of one end user—the retailer—and not in the records of the source of the information—the bank; the customer therefore has the illusion, but not the reality, of having corrected the information.) Must the retailer and the shipper provide access to the recipient of the gift, even though neither has any relationship with him or her? This simple example provides ample illustration of the complexity surrounding the questions of who must provide access and an opportunity to correct to whom.

The Access Trigger. What triggers access? Can consumers file access requests with anyone they think may have personal information about them? Is access triggered if an entity merely possesses or uses personal information, but does not store it longer than necessary to complete the desire transaction? Or must any personal information, once obtained, be stored so that access can be provided?—an ironic result from a privacy perspective. Must access be provided to meaningless or unintelligible information (*e.g.,* encrypted information or a proprietary credit score), or to information where no meaningful opportunity to correct exists (*e.g.*, records of payments that have already cleared or settled)? Must access be provided to information that does not pose any risk of harm (*e.g.,* wholly public record information)? In short, is access to be provided for its own sake or only when it serves some meaningful purpose?. Any proposal that would require that access be provided as a matter of law when it is of no use and serves no purpose is suspect from the start.

The Access-Correction Link. This suggests that access without an opportunity to correct may be of little value. Yet there is a tremendous difference in both the costs and risks associated with access combined with a right to amend, challenge, or delete disputed data, and a tremendous difference among those three options. The silence from access proponents as to exactly what they propose is troubling in light of these vast differences. Must a business open its records to allow consumers to alter at will or to remove information collected by the business as part of a transaction? Who wouldn't want to delete information about debts we owe or misdeeds we have committed? Yet if the right is more limited—for example, access and an opportunity to dispute

the accuracy of data—how will disputes over accuracy be resolved and by whom? Such a requirement seems rife for litigation, and to what end? The specter of endless disputes and nuisance lawsuits over trivial details looms large.

Access Costs and Limits. How is access to be regulated and the cost of access paid for? Will there be limits on access and correction requests? Will spurious claims be restricted? Who will pay for access—only those individuals seeking it or all consumers, through higher prices? Will the price of access be regulated and, if so, by whom and according to what standards?

Certainly some, although it is not clear that all, of these questions may be answered over time. What is surprising and worrying is that many have proposed access legislation without attempting to resolve any of them.

- **Risks**

Even if the unresolved issues are addressed, access and the opportunity to correct personal information online always present significant risks for consumers, as well as for businesses. Five of the most common and important of those risks are:

Authentication. How does an entity required to provide access assure that it is providing access to the right person? This is an extremely complex concern, not just because of the difficulty of authenticating identity, but because all of the measures currently available for doing so require that the individual provide even more personal information about themselves. Consider a practical example: If an individual wants to obtain access online to all of the information collected about him by an online retailer, for example, Amazon.com, how does he authenticate himself to Amazon? He could provide his name and address, but that is hardly sufficient to guard against fraud since both pieces of information are publicly available. He could provide his Social Security number, but Amazon is unlikely to have collected Social Security numbers in the first place. Moreover, Social Security numbers are poor authentication tools since they are used so widely and even printed on checks and driver's licenses. Mother's maiden names are often used as identifiers, but then Amazon is unlikely to collect those so—as with Social Security numbers—it has no way to verify a mother's maiden name even when presented with one. The irony is that not only are none of these techniques likely to be successful, but all require the individual to provide Amazon with more personal information than it would otherwise collect.

Some access advocates suggest that users create a password when they first supply information to a business online. This approach is fraught with problems, not the least of which is few Internet users wish to be bothered with creating a password for a single transaction and usually forget them even when they do. Moreover, the failure to create a password when the information is first supplied presumably makes future access impossible. Finally, this so-called solution, even if it worked, would only apply when information is first collected directly from the data subject, as opposed to be collected from a third party or observed from the data subject's behavior.

Ironically, those who advocate laws mandating access to and the opportunity to correct personal information overlook the fact that the authentication conundrum is inherent to providing access online. As a result, such laws are likely to create greater problems than they are intended to solve. The risk of giving one individual access to, and an opportunity to correct, another individual's personal information is too horrendous to contemplate. Access then becomes the perfect tool for identity theft, and the government that mandates access the unwitting accomplice of identity thieves.

Greater Data Collection and Centralization. The second inherent risk of access schemes is that they require businesses to collect, store, and centralize more—as opposed to less—personal information. For example, as illustrated above, to maintain the tools necessary to authenticate the identity of an individual seeking access, the business is likely to have to seek and store more personal information, such as Social Security number or mother's maiden name, than might otherwise be necessary. Even more troubling, many access proposals require that the business provide the consumer with online access to *all* of the personal information maintained about him or her, even if that information is not normally centralized or accessible via the Internet. As a result, businesses would be compelled as a matter of law to bring together disparate sets of information—to engage in the very act of "profiling" that privacy advocates abhor—and then to make that new "super" database available via the web and therefore subject to viruses and hackers. Some access proposals would even require that businesses retain personal information that they would otherwise have destroyed, just so they can provide access to it at a later date. All of these have the effect of greatly increasing the volume, centralization, and vulnerability of personal data.

The Cost of Access. Few access proposals pay serious attention to the potential cost of providing access and an opportunity to correct personal data. We have already considered the potential costs to consumers in terms of greater data collection and the potential for wholesale identity theft. But the cost of access will also be measured in very real economic costs, reflected in reduced service and convenience and higher prices paid by consumers. In 1995 the European Union adopted a sweeping data protection directive that included, among many other requirements, a right of access to personal data.[6] The British Bankers' Association has calculated the cost of a single institution providing one customer with "a simple and straightforward report" under that law to be "in excess of £150"[7]—about $255 according to the exchange rates in effect at that time. But we don't have to look that far for very practical examples of the cost of providing access. The experience of the federal and state governments in the United States of complying with access and privacy laws to which they are subject shows not only that providing access costs hundreds of millions of dollars and consumes tens of thousands of worker hours each year, but also results in a high volume of litigation over the terms of access and the need for, and adequacy of, corrections.

---

[6]Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281).

[7]*The Home Office Consultation Paper on the Implementation of the EU Data Protection Directive—The British Bankers' Association Response*, Annex I (Costs).

All of the costs associated with requiring that businesses provide access and an opportunity to correct personal information are increased exponentially if that requirement is extended to information collected offline, and increased still further if extended to providing access offline.

The Value of Access and Correction. The fact that mandated access is expensive would pose less of an objection if it were certain to be of sufficient value to warrant the expense, but, as we have already seen, many proposals would guarantee access even when the access was of no value, and involved information not subject to correction, or information that could not be used to cause any harm to consumers. Is the high cost of access justified if purely for psychological benefit?

We might think about the value of access from two additional perspectives. First, why do so many access proposals extend only to information that can be provided online and perhaps only to information collected online? Is this distinction between the online and offline worlds tenable anymore? And why only to commercial users of information—isn't there an equal or greater risk posed by not-for-profit organizations, political campaigns, and individuals who comprise the greatest percentage of hackers and identity thieves? Why must the New York Times provide access to its information storehouses, but not AARP? Why must Time magazine, but not Consumers Union?

A second and even more frightening perspective recognizes that the majority of Americans today admit to cheating on their taxes, lying on resumes, and otherwise deceiving their fellow citizens. Given these facts, is there any reason to suppose that access and an opportunity to seek correction of allegedly false information is going to be used to *increase* the accuracy of stored personal information or rather to *distort* that data to reflect the individual's preferences?

The Constitution. The Constitution says nothing about the privacy of information collected and used by private entities, but a great deal about the value and protection of information. Guaranteeing a right of access to stored personal information, much less an opportunity to alter that information, interferes as directly with cherished free speech rights as requiring that organizations disclose their membership lists, a requirement that the Supreme Court has repeatedly found unconstitutional.[8] Similarly, the Court has consistently and steadfastly declined to allow liability for information just because it is false; individuals aggrieved by such information must also show that the information was used, with a requisite level of negligence or recklessness, to cause them harm.[9] Even when the information involved is intensely personal, the Court has consistently declined to restrict its use. The Court has struck

[8]NAACP v. Alabama, 357 U.S. 449 (1958). Communist Party of the U.S. v. Subversive Activities Control Board, 367 U.S. 1 (1961); Scales v. United States, 367 U.S. 203 (1961); Noto v. United States, 367 U.S. 290 (1961).

[9]Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988); Time, Inc. v. Hill, 385 U.S. 374 (1952).

down laws restricting the publication of confidential government reports,[10] and of the names of judges under investigation,[11] juvenile suspects,[12] and rape victims.[13]

These strictures apply irrespective of whether the speaker is an individual or an institution. Even wholly commercial expression is protected by the First Amendment. The Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a "substantial" public interest, and that the intrusion "directly advances" that interest and is "narrowly tailored to achieve the desired objective."[14] Both courts and the Federal Trade Commission itself have recognized that sales of personal information to third parties are entitled to this same level of constitutional protection.[15]

These limits—while troubling to some—reflect the extraordinary protection that the First Amendment accords to the privacy of individuals and to the groups in which they associate. The First Amendment protects the privacy of every person to think and to express his or her thoughts freely. It therefore fundamentally blocks the power of the government to intrude into the expressive process—the process by which we collect, assemble, and disseminate information—even in order to protect the privacy of other individuals. As a result, the First Amendment restrains the power of the government to control expression or to facilitate its control by private parties in an effort to protect privacy. Those who ignore these constitutional protections put at risk not only freedom of expression, but also the constitutional protection for individual privacy as well.

Conclusion

U.S. consumers today have unparalleled access to the current information (such as account information) we share in common with the businesses with which we deal. We have significant legal rights to obtain access to (in many instances, without charge), and an opportunity to correct, data about us that is in fact private information and that is used—or could reasonably be used—to grant or deny us a benefit, such as credit. This system of market-driven access, backed up with legal rights when necessary, has created a combination of unprecedented openness, service, convenience, and economic prosperity that is the envy of the world.

Some private advocates and government leaders, however, would like to go further and mandate access in the online environment and, for some, in the offline environment as well. These proposals are not only ill-formed, leaving unresolved many of the key issues about the

---

[10]New York Times Co. v. United States, 403 U.S. 713 (1971).

[11]Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978).

[12]Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

[13]Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

[14]Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557, 566 (1980); Board of Trustees v. Fox, 492 U.S. 469, 480 (1989).

[15]*Fair Information Practices in the Electronic Marketplace*, supra at 25 (dissenting statement of Commissioner Orson Swindle).

cost and benefits of such access, but they also inherently pose significant risks to our privacy, the services and convenience we value, and to our constitutional values. They raise the specter of undermining the very privacy they are designed to facilitate and of turning the government into the unwitting partner of identity thieves.

Reasonable, targeted access to personal information serves everyone's interests. Proponents of going further—to mandate access that the market does not appear to value and that consumers cannot effectively use—bear a heavy burden of demonstrating both the need and also that the benefits of attempting to meet that need with legislation justify the inevitable risks and costs that such legislation brings.

July 28, 2000
05-000706