THE PRIVACY PARADOX

76th Annual Winter Newspaper Institute
North Carolina Press Association
Chapel Hill, NC, January. 26, 2001

Fred H. Cate[1]

The Privacy Avalanche

The open flow of information is under attack in the United States as never before in an effort to protect privacy. This issue has united the far right and far left, Republicans and Democrats, federal and state governments, the Eagle Forum and the ACLU, even Phyllis Schlafly and Ralph Nader. In the past two years we have seen a flood of privacy legislation, regulation, litigation—including two supreme court cases upholding sweeping privacy laws,[2] and negotiation. And all indicators are that this is only the beginning: The recent privacy avalanche, rather than satiating appetites for restricting the flow of information to protect privacy, has only whet them.

What is most striking about the current political debate and recent regulatory enactments concerning privacy is their sheer irrationality. I am not suggesting that the desire to protect privacy is irrational, but rather that most of the recent enactments impose extraordinary costs and other burdens on consumers and businesses alike, while failing to accomplish that goal. Despite the fact we are dealing with information flows that are critical to our economy and democracy, both government officials and the press have climbed on the privacy regulation bandwagon without pausing to understand those flows, the critical roles they play, and the likely impact of laws designed to restrict them. Consider just five examples of that irrationality.

1. The Absence of Unregulated Harm

Given the huge volume of privacy legislation and regulation, we might anticipate that there are clearly documented privacy harms that current law does not cover. This would seem necessary in any event to justify government action, but especially in the face of the First Amendment's protection for information flows. Ironically, there is virtually no evidence of harmful uses of personal information that do not violate existing law. The National Association of Attorneys General, for example, issued a report on privacy in December that provided eight examples of alleged misuse of personal information by the private sector.[3] In every example, the alleged misuse had been detected and stopped by law enforcement officials under *existing* law. In many of the examples, substantial fines had been paid by the alleged perpetrator.

---

[1] Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; Senior Counsel for Information Law, Ice Miller Legal & Business Advisors, Indianapolis, IN; Visiting Scholar, American Enterprise Institute, Washington, DC.

[2] United Reporting v. Los Angeles Police Department, 528 U.S. 32 (1999); Reno v. Condon, 528 U.S. 141 (2000).

[3] National Association of Attorneys General, *Privacy Principles and Background Draft* (2000).

Perhaps even more surprising is how few examples there are of privacy harms (by which I mean economic loss or physical injury) at all—especially involving the Internet. There is a lot of speculation, but a recent study from the Progress and Freedom Foundation noted that there is "no empirical or quantitative evidence" of privacy harms online.[4] This is why so many legislative hearings on privacy only feature testimony by lawyers and lobbyists, not victims of privacy harms. You can bet if advocates of privacy legislation could find those victims, they would have them in front of the cameras testifying, but the simple reality is that there are precious few of them and often, when their stories are investigated, the alleged harm is unrelated to the collection and use of personal information or already the subject of existing law. Given the prevalence of information flows and the size of this country, the absence of substantiated evidence of privacy harms is noteworthy.

This was the view of the U.S. Court of Appeals for the Tenth Circuit in U.S. West, Inc. v. Federal Communications Commission, which the Supreme Court in June 2000 declined to review, when it struck down the rules of the Federal Communications Commission requiring that telephone companies obtain explicit consent from their customers before using data about their customers' calling patterns to market products or services to them. The court wrote that the government must show that the information the law would protect as private would inflict *"specific and significant harm*" on individuals: "Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm."[5]

Instead, what policymaking today is based on is unsubstantiated anecdote and fear of the unknown. This may explain the polling data on privacy. While there is extensive polling data that if individuals are asked if they are concerned about privacy they answer "yes," a considerable volume of other evidence suggests that privacy is not day-to-day concern to most Americans. A 2000 survey by Matthew Greenwald & Associates of randomly selected registered voters in five States—California, New York, Massachusetts, Texas, and Washington—found that only 1 percent of respondents mentioned "privacy" as "one of the most important issues or problems that State legislatures should address."[6] This result is particularly noteworthy because those five States were selected for the survey because of the high degree of attention paid to privacy in their legislatures and press. Reports from many legislative staff confirm these findings: Privacy is not an issue that constituents are writing or calling about unless the legislator makes it an issue.

---

4 Paul H. Rubin, *Privacy and the Commercial Use of Personal Information* (2001).

5 U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).

6 Matthew Greenwald & Associates, Views on Privacy and the Sharing of Financial Information Between Business Partners Among Voters in Five States 3 (2000).

This also reflects the actual behavior of most consumers. For example, less than 3 percent of the U.S. population takes advantage of the Direct Marketing Association's Mail and Telephone Preference Services.[7] Financial institutions, retailers, and other businesses report similar or lower figures for their "opt-out" programs. Consumers may respond to privacy polls that they are worried about their privacy, but not so worried that they are doing much to protect it.

The absence of specific, actual harms that new privacy laws are intended to prevent or remedy in a way that existing law does not is a significant issue, because it is only by identifying the harm to which a proposed law responds that a legislator, reviewing court, journalist, or citizen can judge whether the law is necessary, whether it does, in fact, respond to that harm, and whether it is worth the impediment that it inevitably creates to valuable information flows. Without evidence of harm, most proposed privacy laws read very much like solutions in search of a problem.

2. Government as Privacy Protector

Another example of the irrationality of the privacy debate is the role of the government. Privacy advocates' appeal to the government to protect privacy repudiates the longstanding view, reflected in the U.S. Constitution, that the government is more likely to invade, not protect, personal privacy. The constitutional right to privacy, for example, applies only against the government. Jane Kirtley, former Executive Director of the Reporters Committee for Freedom of the Press, has written that the expectation that the government will protect privacy "ignore[s], or repudiate[s], an important aspect of the American democratic tradition: distrust of powerful central government. . . . [W]hen it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart."[8]

Modern opinion polls continue to reflect this view. The 2000 Matthew Greenwald & Associates survey found that the public believes that government is less effective in protecting privacy than financial services companies, health care companies, charities, and retailers.[9] Citizens who report being concerned about privacy consistently rank their greatest concern as fear of government intrusion. And with good reason. Only the government exercises the constitutional power to compel disclosure of information and to impose civil and criminal penalties for noncompliance, and only the government collects and uses information free from market competition and consumer preferences. The General Accounting Office found this past summer that only 85 percent of federal government agency Web sites posted a privacy policy[10] despite a directive more than a year earlier from Office of Management and Budget Director

---

7 Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 20, 1999) (statement of Richard A. Barton).

8 Jane E. Kirtley, "The EU Data Protection and the First Amendment: Why a 'Press Exemption' Won't Work," 80 *Iowa Law Review* 639, 648-49 (1995).

9 Matthew Greenwald & Associates, supra, at 6.

10 General Accounting Office, *Federal Agencies' Fair Information Practices* (GAO/AIMD-00-296R) at 3 (2000).

Jack Lew ordering them to do so.[11] By contrast, the Federal Trade Commission ("FTC") reported in May 2000 that 88 percent of commercial Web sites had *voluntarily* posted privacy policies.[12] A September 2000 Brown University study of 1,700 State and local government Web sites found that only 7 percent posted a privacy policy.[13]

Professor Lillian BeVier has written that the push for the government to protect privacy "seems a little like recommending that the fox, albeit dressed up as a benign and friendly farmer, guard the chickens."[14] Judging from the fact that the government has exempted itself (and the not-for-profit community) from these recent privacy enactments, her argument takes on additional merit. A political campaign sharing the party affiliation of a voter or a not-for-profit group marketing based on the age of a potential member is no less invasive of personal privacy than a financial institution marketing a product or service to customers based on their likely interest and eligibility. In fact, a number of recent federal enactment have made it *easier* for the government to obtain access to personal information held by third parties. Moreover, the government has largely ignored its role in providing identity thieves with forms of identification and its responsibility in protecting its information from unauthorized access or use. There is good reason to doubt both the sincerity of lawmakers who tout privacy legislation, and the efficacy of the legislation they advocate, when lawmakers fail to comply with existing requirements applicable to their own collection and use of information, exempt themselves and other major users of personal information from new privacy laws, and use the legislation to actually enhance the government's ability to search for and seize the most sensitive of personal data.

3. The Cost of Privacy Protection

Third, restricting information flows to protect privacy always, inevitably imposes costs on consumers, businesses, and the economy as a whole by interfering with the benefits, convenience, and reduced prices that robust information flows facilitate. Those costs, however, are needlessly exacerbated when the government regulates *all* uses of information, not just those likely or demonstrated to cause harm. The privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act,[15] whatever their advantages, are certain to prove hugely expensive to implement. The law requires that every business in the country that provides financial services to individuals mail to every one of those individuals a privacy notice, and that it do so again at least annually. That notice must set forth "clearly and conspicuously" how the institution collects and uses information, even though individuals have virtually no legal right to control those uses. Approximately 40,000 financial institutions will be sending as many as 2.5 billion notices to their various customers by June 12, 2001. Individual households will receive an average of 20-50 notices each. Printing and mailing costs alone will be in the 2-5 billion dollar

---

11 Memorandum from OMB Director Lewis Miller (Memorandum M-99-18) (June 2, 1999).

12 Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* at 11 (2000).

13 Darrell M. West, *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (Sept. 2000).

14 Lillian R. BeVier, "Information About Individuals in the Hands of Government: Some Reflections on Mechanisms For Privacy Protection," 4 *William & Mary Bill of Rights Journal* 455, 506 (1995).

15 Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, 1436-1450, title V (1999).

range, if not more. One may reasonably wonder how much consumers will benefit from this onslaught of legal notices, yet it is consumers, in the words of Alabama Attorney General Bill Pryor, who ultimately "pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."[16]

Or consider the final Health Insurance Portability and Accountability Act rules released in December.[17] The rules prohibit the use of information about an individual's health, treatment, or payment for health care, whether oral or recorded, without the individual's express consent. The goal may be laudable and certainly health information is considered by many Americans to be among the most sensitive types of data, but the potential cost to consumers and companies raises significant questions about whether the rules are the best way to protect health privacy. Ironically issued as part of HHS' Administrative Simplification regulations, the release containing the final rules is 367 Federal Register pages long. The required elements alone of the mandatory notice that must be given to consumers before information can be collected or used have been calculated to run nine pages. Although the rules are based entirely on consent, they apply to deceased individuals.[18] And for information to be considered "deidentified"—so that it can be used for medical research without complying with the extensive consent requirements—the information must contain no reference to location more specific than a state (or first three digits of a zip code of certain other requirements are met) and no reference to a date more specific than a year.[19] HHS calculates the compliance cost at $3.2 billion for the first year, and $17.6 billion for the first ten years.[20] Based on the prior and less complicated draft of the rules, health care consulting companies have calculated that the cost will be much higher—between $25 and $43 billion (or three to five times more than the industry spent on Y2K) for the first five years for compliance alone, not including impact on medical research and care or liability payments.[21]

There is no question but that health privacy is important and should be protected as a matter of law. The issue raised by these rules, however, is whether health privacy can be protected as effectively, or even more effectively, at lower cost. And that cost is measured not only in economic terms, but in consumer inconvenience (one family member could no longer pick up a prescription for another family member, because each individual must sign his own consent form), and in potential harm to medical research and innovation.

There are substantive costs to privacy. In a democracy and a market economy, privacy is not an unmitigated good: More is not necessarily better. Privacy facilitates the dissemination of false information, protects the withholding of relevant true information, and interferes with the

---

16 Bill Pryor, Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

17 Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

18 Id. §164.502(f).

19 Id. §§164.514(b)(2)(i)(B)-(C).

20 65 Fed. Reg. 82,761, table 1.

21 Robert E. Nolan Company, Inc., *Common Components of Confidentiality Legislation—Cost and Impact Analysis* (1999); Fitch IBCA, *HIPAA: Wake-Up Call for Health Care Providers* (2000); Barbara Kirchheimer, "Report Predicts Huge HIPAA Price Tag," Modern Healthcare, Oct. 2, 2000, at 48.

collection, organization, and storage of information on which businesses and citizens alike can draw to make rapid, informed decisions.

And there are significant, but largely ignored, costs of privacy protections in the form of increased burdens on consumers—not just in more forms and disclosure notices, but in virtually every aspect of daily life. Consider target marketing, for example. Information-sharing also allows consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested. As a result, information on second mortgages and home improvement services can be targeted only to home owners. Information on automotive products and services are targeted only to car owners. The American Association of Retired People can target its offers only to older Americans, and veteran's organizations can appeal only to people who have served in the armed forces. Political campaigns can target their solicitations to registered members of appropriate political parties.

In the face of laws restricting this use of information, organizations—at least those that survive the increased costs occasioned by not being able to use target marketing—will have to contact households randomly; they will send more unsolicited mail and e-mail and place more telephone calls in an effort to find those people interested in their offer. The public will be peppered with more mail, e-mail, and telephone calls, a higher percentage of which will be of no interest to the recipient. This would truly be "junk mail," because it would have been generated without regard for the recipient's demonstrated interests.

Are laws designed to protect privacy, especially those that respond to no identified harm, worth these costs? That is the question that lawmakers, the press, and the public should be asking.

4. The Fallacy of Consent

Proponents of those laws often argue that all businesses and other organizations need to do is educate consumers about the benefits of information flows, and then those individuals will consent to the collection and use of information about them. The simple, straightforward nature of this argument has made it very powerful, but it is often wrong, for many reasons:

- Unanticipated Benefits—The benefits of personal information are often unanticipated. For example, many retailers collect information about consumer purchases and then access that information so that consumers can return merchandise at many retailers without a receipt, order supplies and replacement parts without knowing the exact model number or specific product information, obtain information about past purchases for insurance claims when fire or other disasters destroy or damage those goods, and receive immediate notification about product recalls and other safety issue. These are tangible benefits that many consumers take advantage of every day. But few consumers would anticipate in advance that they were going to need information about a past transaction for insurance purposes or to order replacement parts. The benefit is exceptionally valuable when it is needed, but often illusory before that time.

- Lack of Consumer Contact—Many of the benefits result from uses of personal information that do not involve the consumer directly. For example, credit bureaus update consumer credit files—the files that are used to obtain rapid, low cost access to credit of all forms—without ever dealing directly with the consumer. In fact, few Americans will ever deal directly with a credit bureau. For the credit bureau to have to establish contact with the consumer every time it needed to collect or use information about him or her would be expensive and burdensome to the consumer. Similarly, most mailing lists are obtained from third parties, not the people whose names are on the list. For a secondary user to have to contact every person individually to obtain consent to use the information would cause delay, require additional contacts with consumers, and almost certainly prove prohibitively expensive.

- Value of Standardized and Third-Party Information—There are many beneficial uses of personal information where the benefit, frankly, is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: Much of its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless. Even when information is not particularly "positive" or "negative," its value may depend on it being complete. Many business monitor accounts for suspicious activity that may indicate fraudulent activity. Often credit card companies will call a card holder whose account has experienced unusual charges to verify that the card has not been stolen. Identifying the unusual requires knowing what is usual and that, in turn, requires access to a complete set of data.

- Consumer Preferences—Most consumers do not want to be deluged with repeated requests for consent. The ultimate result is that consumers will either not consent, and thereby diminish the benefits that flow from information-sharing both for themselves and others, or they will consent to everything, just to avoid further calls and letters and e-mails.

- The Practical Obstacles to Consumer Contact—Conditioning use of personal information on specific consent may also harm consumers because of the practical difficulties of reaching many consumers. Consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. To obtain permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls, and one-third of their customers were denied opportunities to receive information about valuable new products and services.[22]

22 Brief for Petitioner and Intervenors at 15-16, U.S. West, Inc. v. Federal Communications Comm'n, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

- The Interconnectedness of Consent—Many of the beneficial uses of information that consumers now enjoy and to which they have the opportunity to consent, depend on spreading the cost of collecting and maintaining the information on a variety of uses. For example, open government records today are collected, organized, and made accessible to the public by commercial intermediaries. Those records are used for countless socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from "deadbeat" parents and spouses, and many others. In fact, in 1998 the FBI alone made more than 53,000 inquiries to commercial on-line databases for "public record information."[23] The Association for Children for Enforcement of Support uses information from public records, provided through commercial vendors, to locate over 75 percent of the parents they sought.[24] Access to these records is possible, as well as convenient and inexpensive, precisely because commercial intermediaries assemble the information for such a wide variety of other uses. If the law restricted the other valuable uses of public records, or made those uses prohibitively expensive, then the data and systems to access them would not be in place for any use. As a result, laws requiring consent for data use may only create the illusion of consent, because they will lead to consumers having fewer opportunities made available to them to which they can consent.

- Compelled Consent—The opportunity for consent may also be illusory because most organizations will not, and cannot, provide a service or product to a customer without consent. HIPAA, for example, requires that physicians provide extensive disclosures and obtain explicit consent concerning information collection and use prior to treating a patient. If a patient wishes to be treated, he or she must consent. Experience suggests that few people will shop for physicians based on information policies; rather, their decisions about from whom to seek service will be driven by price, location, insurance coverage, specialty, and other considerations. So the billions of dollars that will be spent crafting, providing, and storing consent forms will likely achieve little in terms of enhancing consumer choice or privacy.

- Consumer Ignorance and Lethargy—Even if the request gets through to the intended adult recipient, the most immediate response to requests for consent to use personal information, to judge by extensive business and not-for-profit experience, is that the customers will simply ignore the request. Most unsolicited mail in this country is discarded without ever being read and most unsolicited commercial or fund-raising telephone calls are terminated by the consumer without the offer ever being made. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Even where mail is actually

23 Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Comm. on Appropriations, U.S. Senate, March 24, 1999 (statement of Louis J. Freeh).

24 Hearings before the Committee on Banking and Financial Services, U.S. House of Representatives, July 28, 1998, (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).

> read and the offer appeals to the consumer, lethargy and the competing demands of busy lives usually conspire to ensure that no action is taken. It is difficult to imagine that promises of potential future benefits from information use will command greater attention or activity.

These considerations suggest that simply conditioning the use of personal information on specific consent is tantamount to prohibiting many beneficial uses of information outright, because of the cost of obtaining consent, the extent to which selectivity in the information included undermines its usefulness, the degree to which uses of information are interconnected, and the many impediments to consumers receiving and acting on the request, even when it is in their best interest to do so. What is needed is a better way of balancing the benefits that consumers receive from a robust flow of personal information with individuals' legitimate interest in privacy.

5. Diminishing Privacy Protection

Much of the recent activity concerning privacy ignores the vital role of consumers in protecting our own privacy, and too often diminishes our capacity to do so. The focus on new privacy laws teaches consumers to worry about privacy and to put our trust (and our privacy) in the hands of the government, when we all know that law is not sufficient to protect privacy. For example, law does nothing about information users who operate offshore (which a majority of Web site operators do) and nothing about users who operate outside of the law.

Many privacy proposals also distract consumers from the practical steps that individuals—and often only individuals—can take to protect our own privacy. Take identity theft for example. Despite all of the bills that have been introduced to combat identity theft, the most effective means continue to be those that individuals take to protect ourselves: keeping a close watch on account activity; reporting suspicious or unfamiliar transactions promptly; properly destroying commercial solicitations; storing valuable documents securely; protecting account names and passwords; and never disclosing personal information to unknown callers. Moreover, while legislation is focused on protecting against identity theft by strangers, the majority of identity theft cases appear to involve friends and family members. The practical, specific steps that individuals can take, in contrast to pending laws, protect us against both strangers *and* friends and family members.

Government intervention also often interferes with the considerable privacy protection available from technologies, competitive market offerings, and self-help. Most of the pending bills to prevent identity theft would restrict the use and disclosure of Social Security Numbers. This highlights the conundrum that efforts to prevent identity theft inherently pose. One of the major issues concerning identity theft today is how to accurately separate data about one individual from data about another. This is made all the more difficult by the fact that approximately 16 percent of the U.S. population—about 42 million Americans—changes addresses every year; there are approximately 2.4 million marriages and 1.2 million divorces every years, often resulting not only in changed addresses, but also changed last names; and, as

of 1998, there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses.[25]

The only reliable way to date to ensure that information about one consumer is not erroneously provided to another consumer or added to another consumer's file is to organize those files by SSN. Just a single segment of the modern economy—consumer reporting agencies, i.e., credit bureaus—processes 2 billion pieces of personal data on 180 million active consumers every month. Identifying those data by SSN (together with other personal information) is the only reliable way of ensuring that they are attributed to the right person. Yet this is precisely what proponents of legislation designed to restrict the use of SSNs want to stop. They argue that such legislation is necessary to limit the availability of SSNs in the market and thereby reduce their availability for use in identity theft. The commercial use of SSNs, rather than being a significant source of information for identity thieves, is often a significant protection *against* identity theft.

Similarly, many businesses are expanding their account monitoring to detect fraud. Account monitoring has proven to be one of the most effective methods for identifying fraudulent transactions and victims of identity theft, especially when that monitoring occurs across accounts and across affiliates, so that the merchant has more comprehensive and precise knowledge of transaction patterns. Even the most ardent privacy advocates argue that account monitoring is critical to preventing and detecting identity theft. Yet a number of pending privacy laws threaten to restrict the ability of merchants to use this identity theft detection strategy or to condition account monitoring on consumer consent. As a result, the government becomes the unwitting accomplice of identity thieves.

Conclusion—The Role of the Press

To date, the press, far from exposing these and other irrationalities, has helped to contribute to them. With few exceptions, journalists have overwhelming climbed on the privacy bandwagon, weaving together unsubstantiated claims of privacy harms with support for legislation that often would not respond to those alleged harms. In California, every major newspaper in the state editorialized in favor of pending privacy legislation this past year, with many calling for more serious legislation. The press has almost wholly bought into the claim that privacy is a simple issue that just requires that every one be given a chance to consent. And you have done so with a breathtaking disregard for how significantly privacy laws would affect your reporting and the values that reporting serves. Even when states have directly threatened to close the public records on which you depend, only a handful of papers have objected to privacy laws.

So let me conclude with four observations/recommendations that focus directly on the press.

---

25 Use and Misuse of Social Security Numbers, Hearings before the Subcomm. on Social Security of the Comm. on Ways and Means, U.S. House of Representatives, May 11, 2000 (statement of Stuart K. Pratt, Vice President, Government Relations, Associated Credit Bureaus, Inc.).

First, recognize that the press is not exempt from the privacy avalanche; in fact, you may be one of its primary targets. For example, the 1994 Drivers Privacy Protection Act[26] restricts the disclosure of name and address information—the least private and most widely shared of all information—from motor vehicle records. Although the Act was enacted in response to the 1989 murder of actress Rebecca Schaeffer, who was stalked by an obsessed fan using information provided by a private investigator from her California Department of Motor Vehicles record, the law restricts the access by the press and the public to motor vehicle records, but not that of private investigators.

Second, when you write and editorialize about privacy laws, consider their impact on the press and the public. That impact is especially clear in the case of public records. Access to public records is essential for journalists and other researchers to gather information and inform the public about matters of public importance. In fact, a recent study by Indiana University Knight Journalism Fellow Brooke Barnett found that journalists routinely use public records not merely to check facts or find specific information, but to actually generate the story in the first place. According to that study, 64 percent of all crime-related stories, 57 of all city or state stories, 56 percent of all investigative stories, and 47 percent of all political campaign stories rely on public records. Access to public record databases is "a necessity for journalists to uncover wrongdoing and effectively cover crime, political stories and investigative pieces."[27]

But don't ignore the impact of laws and regulations addressing information collection and use by the private sector. These laws also threaten the ability of the press and the public to obtain critical information about important events and issues. For example, both the Society for Professional Journalists and the Reporters Committee for Freedom of the Press have noted the serious threat posed by the HIPAA privacy regulations to reporting about health-related matters.[28]

Third, bring the same critical assessment to proposed privacy laws and regulations that you do to other important subjects. Hold the feet of lawmakers and privacy advocates to the fire with the same vigor and skepticism that you show to business leaders. What purpose does the law serve? Will it actually accomplish that purpose? At what cost? Is it consistent with the constitution? Does the law apply to political campaigns, lobbyists, consumer advocacy groups, and not-for-profits? Ask the tough questions—not only about what is under active consideration but also about what is not. What should the government be doing to really enhance citizen

---

26 Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).

27 Brooke Barnett, Use of Public Record Databases in Newspaper and Television Newsrooms (2000) (unpublished ms.).

28 Society for Professional Journalists, *Medical Privacy Rules Ignore Public's Interest, Media's Role* (press release) (Dec. 22, 2000); *Comments of the Reporters Committee for Freedom of the Press Concerning RIN 099–AB08, Standards for Privacy of Individually Identifiable Health Information* (Feb. 17, 2000).

privacy? Why hasn't the government made the promise of centralized reporting of identity thefts a reality? Why is it so hard to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief? How much funding has the legislature appropriated to enforce existing privacy laws?

Finally, educate the public about privacy, the costs and benefits of protecting privacy, and the tools available to every citizen to protect his or her own privacy. Inform us about the 800-numbers we can call to be removed from mailing lists and prescreened offer lists, how to use the technology already in our Internet browsers to protect against unwanted profiling and data collection, and about the steps that we—and often only we—can take to protect our own privacy. Greater citizen understanding of the importance of both privacy protection and other goals and values (such as open public records and robust information flows) with which privacy protection inevitably interferes, is essential. These are not easy or simple issues, but they are critical ones, affecting not only the vital activities of the press, but the very livelihood and liberty of us all.

Thank you.