POLICY BACKGROUNDER No. 156
For people with limited time and a need to know.

For Immediate Release
April 27, 2001

The Evolving Technologies of Internet Privacy

By Gregory F. Rehmke

Two dynamic Internet software industries are emerging. One is the data-mining industry, producing software tools that firms use to analyze consumer behavior and preferences on the Internet. The other is the privacy software industry, whose products are designed to stop some or all of this individual information from being collected and analyzed.

Entrepreneurial firms are rushing to offer a variety of products to serve Internet advertising and data-gathering firms on the one hand and individuals and groups with privacy concerns on the other. The competitive marketplace is searching for the amount of privacy that people want and are willing to pay for. Microsoft's announcement of the new privacy features planned for the next release of its Web browser, Internet Explorer, highlights the growing response of the private sector to concerns about privacy on the Internet. These concerns have to do not only with privacy from businesses and other individuals but also with privacy from government.

"Most new privacy legislation proposes to interfere with the development of new technologies."

More than a score of privacy-related bills have been introduced in the 107th Congress, several of them specific to Internet privacy. Some propose restrictions on the federal government's own use and potential abuse of private information about American citizens. Most of the new legislation, however, proposes to legislatively interfere (or further interfere) with the development of information and privacy technologies in the private sector.

Customer Preferences and the Internet

For millions of Americans the Internet is a tool for exchanging e-mail, researching distant databases, and purchasing books, tickets and a wide array of other products and services.

But the rapid expansion of electronic databases, e-mail and Internet commerce has dramatically lowered the cost of information about *people* as

ISBN #1-56808-104-9

well as about products. Internet users are amazed at the amount of information about products and services available online. This same electronic magic can turn every online search and every purchase into new database records about the person who made that search or purchase.

This is accomplished primarily with "cookies," little data files that are saved to an Internet user's computer when the user visits a Web site. Cookies store information such as what the computer user does on that Web site and what other Web sites the computer user visits. The next time the user visits the Web site, the cookie makes it possible for the Web site to tailor what the site offers based on information about the user's interests.

"Cookies make it possible to tailor what a Web site offers based on information about the user's interests."

Imagine if Wal-Mart were to record the movements of individual shoppers in its stores, noting where they stopped to look at items and what they picked up and put back. Wal-Mart could use this information to improve product placement and display designs. But in the end an individual Wal-Mart store looks the same to each customer — even though each customer has different interests and preferences. Perhaps some futuristic Wal-Mart will be able to quickly rearrange shelves as customers walk down the aisles in order to offer goods according to each customer's known preferences (maybe, for example, a product you picked up and considered buying would turn up on shelves again and again as you walk through the store).

Until that time, however, people can only get such individualized treatment at online stores and only if online stores are allowed to gather information about customers and visitors to their Web sites. Amazon.com offers such personalized service. Return visitors to the Amazon Web site see books recommended on the basis of past books they have considered or purchased.

Netflix (www.netflix.com) offers DVD movie rentals on its Web site, and members can rate dozens of movies as well as choose the DVDs they want mailed to them. The Netflix software remembers the ratings and which movies have been rented, and suggests movies that its software determines users might enjoy.

Visitors to small-town video-rental stores can enjoy similar benefits from conversations with store employees who over time suggest movies. Shoppers in small stores in small towns are more used to being observed by store owners and employees concerned about providing good service. With analysis technology, online stores provide aspects of this small-store attention and can combine it with large-store selection and economies of scale.

PC Magazine recently reviewed the latest data-mining software.[1] Analytics, e-marketing and what is called personalization software enable firms to identify shopping and other traits of consumers and adapt their Web sites to the interests and preferences of users. [See Table I for a listing of personalization software.]

TABLE I

PC Magazine Table of Personalization Software

Company	Personalization Features	Firms Using Software
Art Technology Group www.atg.com	User profiling and content targeting. Partners with filtering companies.	John Hancock Funds, Smith & Hawken, Sony Online Entertainment
Blaze Software www.blazesoft.com	Rules-based engine for developing and serving targeted content.	CitiGroup, UPS, U.S. Treasury Dept.
BroadVision www.broadvision.com	Rules-based engine for developing and serving targeted content.	Credit Suisse Group, Fingerhut, Motorola, Nortel Networks, Sears
Manna www.mannainc.com	Collaborative filtering and rules-based engine for serving targeted content in real time.	Get-Outdoors.com, GourmetMarket.com, saleoutlet.com
Net Perceptions (Company info) www.netperceptions.com	Collaborative filtering engine for developing targeted content and product recommendations.	Amazon.com, CDnow, JCPenney, Mattel

Adapted from: http://www.zdnet.com/pcmag/stories/reviews/0,6755,2684762,00.html

Opting out of the Personalized Technology World

People who have lived in small towns are used to diminished privacy. They are used to knowing the people they buy magazines from in the corner store and borrow books from in the local library. But most Americans in cities and suburbs make their purchases from people they don't know. And for them this era of electronic observation is new and sometimes troubling.

"Not everyone wants data 'mined' from personal browsing and purchasing behavior."

Not everyone wants data "mined" from their personal browsing and purchasing behavior. Many who grew up in small towns didn't like having much of the information they considered personal known by everybody in town. Similarly, many now resent the electronic gathering of information about what they have purchased and the sites they have visited on the Internet. They don't like the idea that companies and advertisers are collecting the crumbs of information they leave as they move from site to site, execute searches, research topics and make purchases.

For people who are willing to trade the "personalized" service on Amazon.com and other Web sites in exchange for anonymous surfing (and

even anonymous shopping!), there are a growing number of products and services. Web-browsing privacy can be protected by using anonymous Web browsers like SafeWeb, e-mail encryption software like HushMail and cookie managers like Cookie Cruncher [see Table II].

Of the new firms announcing software tools that allow for anonymous Internet browsing, SafeWeb, IDZap and ZeroKnowledge received the highest ratings from *PC Magazine*.

- If people don't want anyone to observe their Web browsing they can log onto www.safeweb.com and from there search Web sites without being watched (unless someone is standing behind them watching!).
- IDZap offers a similar service, hiding one's identity from the Web site being visited.
- ZeroKnowledge Systems features an extensive set of software tools that allow for anonymous e-mail and Web browsing for a number of users.

Some of these privacy tools, cookie management tools in particular, are featured in the latest version of Platform for Privacy Practices (P3P) standards developed by the World Wide Web Consortium (W3C). The biggest privacy news is Microsoft's plan, mentioned above, to include P3P in the next release of its Web browser, Internet Explorer. P3P is a set of standards for both Web browsers and Web sites that allows users to indicate their privacy preferences and to limit the release of personal information to Web sites that agree to keep that information private.[2]

"New software tools allow anonymous Internet browsing and e-mail encryption."

TABLE II

The Electronic Privacy Information Center's Online Guide to Practical Privacy Tools

(partial listing)

Snoop Proof Email	Ziplip.com, SafeMessage, Private Messenger, HushMail, Mail2Web.
Surf Anonymously	Freedom, I Can See You, BrowsInfo, The Anonymizer, Proxymate, the Cloak, Rewebber, Idzap, Aixs, SafeWeb
HTML Filters	Junkbusters, Proxomitron
Cookie Busters	Cookie Cutter, Cookie Jar, Cookie Crusher, Cookie Cruncher, MagicCookie Monster

http://www.epic.org/privacy/tools.html

Critics of private-sector Internet privacy technologies have complained that they are hard to use and that most people won't bother with them. Microsoft's plan to include P3P in Internet Explorer would seem to address this concern, since it will be fairly easy for people to tell Explorer what their privacy preferences are and let it certify the privacy practices of Web sites. However, the Electronic Privacy Information Center (EPIC) and some other privacy advocates are not happy with P3P and Microsoft. EPIC contends that P3P "fails to comply with baseline standards for privacy protection."[3] It argues that P3P will just make the collection of information more systematic and insists that there is a "right of individuals to control the collection, use and dissemination of their personal information that is held by others."

"Individuals don't 'own' information about themselves."

One problem with claiming that individuals can and should "own" the information others have about them is that it is obviously not true. We don't and can't own our reputations, for example. There are two parties to each transaction and unless there is an agreement or common law rule about keeping information about a transaction private, both parties possess the information about the transaction. Some information is sensitive and some clearly isn't, and traditions and standards have evolved to distinguish between them.

Subscribers to *Time* magazine shouldn't be surprised to begin getting solicitations from other magazines, especially other magazines published by AOL Time Warner. (Interestingly, any legislation designed to prevent firms from selling information about consumers to other firms would tend to harm small companies more than large conglomerates, since the conglomerates could still transfer information among their separate companies — which would probably lead to further "clarifying" legislation.)

Some privacy advocates fear that consumers will be manipulated by corporations that know "too much" about their purchasing patterns. The concern is that people will buy things they really didn't want until some crafty advertisement made them want it. Somehow, goes this reasoning, the collection of more and more information on the Internet will make this problem even worse. Of course, such claims can also be made of books, museums and operas — we are unlikely to know how enjoyable they are until we discover they exist.[4] It's true that we are unlikely to purchase products we don't know about, but that doesn't mean we will blindly buy whatever product is advertised. The traditional view of advertising, according to economist Israel Kirzner, "saw advertising as a fundamentally baneful phenomenon, thwarting the tendency of competitive markets to allocate resources efficiently." However the emerging view, according to Kirzner, sees advertising as playing an "essential and constructive role [in] the functioning of markets."[5] We live in a world of goods and services that must compete for our attention. We don't have enough time to learn about every good and every

experience available to us. Companies look for ways to get the attention of people who might want to buy their products and services. And past purchases are clues about people's preferences for future purchases.

Developing Privacy Standards

Technologies evolve in unexpected directions. Personal computers connected to networks of computers form an *Inter*net that speeds information flows. But unlike newspaper, radio and television technology, Internet technology is interactive and information flows in both directions

The virtual world of cyberspace confuses our sense of privacy. When users on home computers browse through the Wal-Mart Web site, should this interaction be considered like paging through a Wal-Mart catalog at home or like walking through a Wal-Mart store down the street or in Arkansas? Is Wal-Mart sending the information into homes, or are we sending our virtual selves out into virtual shopping malls?

"Acceptable standards of behavior toward information gathered in commerce are developing, and will likely evolve over time."

Either way, the interaction is voluntary. We are welcomed as we enter the virtual Wal-Mart, or we invite an interactive Wal-Mart catalog into our home and onto our desktop. The information generated by this voluntary interaction is obviously available to both parties. We can tell others what we saw on display in the online Wal-Mart, and Wal-Mart can study what we looked at — what products and displays we lingered over, what pathways we took while clicking through their store.

What are acceptable standards of behavior toward private information gathered in commerce? These standards are developing according to what people consider just, fair and efficient. And these marketplace standards will likely evolve over time.

Major privacy certification firms TRUSTe and BBBOnline [see Table III] have developed privacy standards, certify sites that promise to adhere to them and adjudicate (privately) disagreements and disputes. These standards are not settled, but the process is transparent rather than secret and bureaucratic. Some firms and organizations criticize TRUSTe, for example. The EPIC Web site describes some disagreements, and the SafeWeb site claims that the TRUSTe symbol does not guarantee visitors' privacy. (And surprise! They claim using SafeWeb does.)

Government Threats to Privacy

The increasingly robust private-sector privacy standards and privacy software tools contrast sharply to the vague and hypocritical efforts of governments (here and in Europe) to promote top-down privacy standards for Web sites.

TABLE III

Seals of Approval for Privacy Policies

Better Business Bureau Online	**Privacy Seal Program** Helping Web users identify companies that stand behind their privacy policies and have met the program requirements of notice, choice, access and security in the use of personally identifiable information.
TRUSTe Building a Web you Can Believe In" ™	**The TRUSTe program** enables [firms] to develop privacy statements that reflect the information gathering and dissemination practices.

Failing to Follow Internet Privacy Policy. When the inspectors general of all U.S. federal agencies began auditing government Web sites, audits of the first 16 agencies disclosed dozens of violations of administration privacy policies.[6] Many government sites that had been banned from using cookies were using them. Some sites that collected personal information did not have a posted privacy policy, and some collected e-mail addresses without the user's knowledge.

"Federal government Web sites have not been following privacy rules being pushed on the private sector."

The Federal Trade Commission was embarrassed when it was reported that the stringent privacy rules it was pushing on private sector e-commerce sites were not even adhered to by federal government Web sites.[7] A General Accounting Office study found only 3 percent of audited government sites followed the FTC's proposed rules. The other 97 percent, including the FTC's own Web site, used the same "opt-out" policies that most private Web sites used and which the FTC was trying to ban.

The White House Office of National Drug Control Policy allowed advertisers on its Web site to store cookies on visitors' computers.[8]

The *Wall Street Journal* reported recently on the ironic results of detailed privacy regulations in the European Union.[9] Consumers International, a United Kingdom-based consumer organization, surveyed over 700 major Web sites in the E.U. and U.S. where people were likely to be asked for personal information. The results must have surprised privacy advocates who complain about the lack of privacy regulation in the U.S. and call for "stronger" top-down privacy regulations like those passed by the European Commis-

sion. The *Journal* reported that "Internet users' privacy is better protected in the U.S. than in Europe, despite the raft of privacy regulations that have been approved by the European Commission over the past five years." [See Table IV.]

The article further noted, "The U.S. model of voluntary self-regulation of the use of private data collection online appears to work better."

"Despite a raft of privacy regulations in Europe, Internet users' privacy is better protected in the U. S."

Fighting Individuals' Internet Privacy. In *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*,[10] Steven Levy describes frantic National Security Agency (NSA) efforts to keep strong encryption technology inside the "triple fence" of NSA headquarters. Gradually through the 1980s and 1990s outside cryptographers developed private-sector encryption software, and entrepreneurs tried to make these software tools popular. Federal government agencies tried everything they could to stop the release of this technology. And had they been successful, private citizens today would not be able to protect their communications over the Internet. (Or at least the public would not have been allowed strong enough encryption to keep their communications private from government snoops.)

TABLE IV

Consumers International Survey of U.S. Versus E.U. Web Site Privacy Protection Policies

What compulsory and optional information did U.S. and European Web sites collect? (from a survey of major U.S. and European Web sites conducted by Privacy International).

	Compulsory		Optional	
Personally Identifiable	U.S.%	E.U.%	U.S.%	E.U.%
Name	50	74	44	24
Address	38	61.5	38	27
Phone	36	35	34	41
Credit Card Debts	1	10	4.5	7
Demographic Data				
Postcode	37	57	42	27
City	37.5	58	40	26
Birth Date	10	15	10	12
Gender	1	5	1	2

From Privacy@net: An international comparative study of consumer privacy on the Internet, published by Consumers International (www.consumersinternational.org)

The government was concerned because it believed cheap or free encryption software would allow criminals, terrorists and tax-evaders to encrypt their e-mail and Web browsing so powerfully that even the FBI, CIA and NSA would not be able to decode them. That *may* be okay for average citizens, but what about criminals and potential terrorists? This is a reasonable concern but not one that is easily dealt with. Just as strict gun-control laws could help keep guns out of the hands of everyone except criminals, strict encryption-control laws could restrict use by everyday citizens but not computer-literate criminals and terrorists.

"Federal agencies have tried to keep strong encryption technology away from private citizens."

The FBI Carnivore project was designed to sift through e-mail and Internet browsing by tapping into Internet Service Providers' hardware. Since most people don't bother to encrypt their e-mail correspondence, this allows the FBI to execute searches once they have proper warrants that identify the people whose e-mail and Internet access they wish to tap. Critics of Carnivore have been concerned that its technology was likely to allow other people's e-mail to be searched at the same time but without benefit of warrants.

The FBI responded by addressing the most glaring problem with their Carnivore project — its name. So now it is called DCS1000, which stands for "digital collection system."

Invading Privacy On and Off the Internet. The private sector has moved rapidly to provide an expanding array of privacy-protecting products and services — none of which would have been available to consumers if the government had had its way in keeping encryption technology classified. Now many people want Congress to step in and regulate privacy standards in the private sector. But these standards are a moving target, and no one can know where they will be in one, three or five years (unless they are hit with heavy-handed regulation, in which case innovative privacy technologies will likely migrate overseas). Further, there are valid questions about the will of government to protect private-sector privacy.

James Plummer, in an article in *Ideas on Liberty*, notes that the real privacy problems are not with private-sector activities anyway but with those of the public sector, both on the Internet and elsewhere.[11] Plummer lists 10 major privacy concerns that come from the public sector:

1. Federal Web sites (97 percent of which violate FTC-promoted privacy standards).

2. Mailboxes (the Post Office now requires those who want private postal boxes to show two forms of identification).

3. Brady Law databases (the FBI is creating a national database of firearm owners).

4. "Know Your Customer" (Congress is pushing banks to snoop on customers and report any "abnormal" activity to the government).

5. National ID (such schemes are pushed for health, immigration reform and other reasons every few years).

6. Wiretaps (the 1994 Communications Assistance for Law Enforcement Act (CALEA) forced phone companies to help track a growing amount of phone and cell phone information).

7. Internal Revenue Service audits (information in our tax returns is supposed to be private, but it is available to other federal agencies and not well protected from electronic intrusion, according to the General Accounting Office).

8. Filegate. Another oldie but goodie, this one is still having repercussions today. When more than 900 FBI files of Republican political appointees mysteriously appeared in the White House, the Clintons blamed a "bureaucratic snafu." Depositions by Linda Tripp and others taken in the ongoing civil litigation[12] have revealed that information from the files was copied into White House databases for later use.

9. Echelon (a global automated eavesdropping operation run by the U.S., U.K., Canada, Australia and New Zealand that only the French seem to oppose, because they have their own).

10. DCS1000 (formerly Carnivore).

Conclusion: Searching for Balance

No one knows or *can* know the ideal degree of privacy people desire, or how to achieve it, or how that degree of privacy preference may change over time. So what we want is a process for discovering such preferences and enforcing rights and obligations where they exist.

These standards don't have to be invented or mandated by new legislation. Accepted privacy standards already exist in the business world for the work of doctors, accountants, lawyers and other professionals. Privacy advocates claim these same strong standards should be forced onto the Internet. But there has long been a difference between how information is treated in connection with the provision of services and in connection with the sale of products. Doctors generally examine us and advise us in private, not in a department store or at a check-out counter. But if few of us bother to keep secret what we purchase in grocery or department stores, why is it so important to keep these transactions secret on the Internet?

"There has long been a difference between how information is treated in the provision of services and in the sale of products."

Sometimes people may not want others to know where they shop or what they purchase or what they copy to their computers. This is especially true in totalitarian countries, where people justly fear their own government (two of the founders of SafeWeb are from China and Iran). Unfortunately, the design of the Internet, like the design of early telephone systems with party lines, allows Internet lurkers to observe Web browsing and e-mail.

State and federal governments are ready to jump in with legislative mandates to try to protect Web browsing and e-mail privacy. But governments have not even been very good at observing their own privacy rules.

Technological developments have created the vast network of databases and interactive communication that is raising many of the concerns about privacy. New software will increasingly make it feasible for individuals to set their own flexible limits on how much information about their Web-use activities they share with others. They will be less able to control generally available information about themselves, just as they were in the days before technology made that information available electronically. But technology, not legislation, can make it possible for individuals to strike a balance on how much they want to participate in information sharing in this Information Age.

"Technology, not legislation, can allow individuals to strike a balance between privacy and sharing information about themselves."

Gregory F. Rehmke is a program director at the Foundation for Economic Education.

NOTE: Nothing written here should be construed as necessarily reflecting the views of the National Center for Policy Analysis or as an attempt to aid or hinder the passage of any bill before Congress.

Notes

[1] *PC Magazine,* special privacy issue, January 16, 2001.

[2] For information on the Platform for Privacy Practices, see http://www.w3.org/P3P.

[3] "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy," Electronic Privacy Information Center, June 2000, p. 2, available at www.epic.org/Reports/prettypoorprivacy.html.

[4] I would argue that in the case of museums and opera it is the relative lack of advertising that keeps most of the public unaware of the deeply satisfying experiences these and other arts offer. The Bellagio Hotel in Las Vegas — which has one of the few for-profit art museums in the country (if you like a painting, you can buy it!) — draws many times the people as similarly-stocked non-profit museums.

[5] Robert Ekeland Jr. and David Saurman, *Advertising and the Market Process* (San Francisco, Calif.: Pacific Research Institute, 1988), p. xv.

[6] Nancy Zuckerbrod, "Report: Privacy Not Protected Online," Associated Press, April 17, 2001; and "IG Reports on Internet Data Collection," news release, U.S. Senate Governmental Affairs Committee, April 17, 2001.

[7] U.S. General Accounting Office, "Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles," Letter to Reps. Dick Armey and W.J. Billy Tauzin, September 11, 2000.

[8] Mark Davis, "Is the Drug Czar Skirting the Law?" *Insight*, September 18, 2000.

[9] "U.S. Privacy Protection Model Works Better, According to Report," *Wall Street Journal*, February 20, 2001, p. B11.

[10] New York: Viking Press, 2001.

[11] James Plummer, "Ignoring Real Privacy Problems," *Ideas on Liberty*, February, 2001, p. 44.

[12] These are available at www.judicialwatch.org.

About the NCPA

The National Center for Policy Analysis is a nonprofit, nonpartisan research institute founded in 1983 and funded exclusively by private contributions. The mission of the NCPA is to seek innovative private-sector solutions to public policy problems.

The center is probably best known for developing the concept of Medical Savings Accounts (MSAs). The *Wall Street Journal* called NCPA President John C. Goodman "the father of Medical Savings Accounts." Sen. Phil Gramm said MSAs are "the only original idea in health policy in more than a decade." Congress approved a pilot MSA program for small businesses and the self-employed in 1996 and voted in 1997 to allow Medicare beneficiaries to have MSAs.

Congress also relied on input from the NCPA in cutting the capital gains tax rate, in creating the Roth IRA and eliminating the Social Security earnings penalty. These proposals were part of the pro-growth tax cuts agenda contained in the Contract with America and first proposed by the NCPA and the U.S. Chamber of Commerce in 1991. Two other tax changes — an increase in the estate tax exemption and abolition of the 15 percent tax penalty on excess withdrawals from pension accounts — also reflect NCPA proposals.

Another NCPA innovation is the concept of taxpayer choice — letting taxpayers rather than government decide where their welfare dollars go. Legislation to create taxpayer choice at the state level was sponsored last year by Reps. John Kasich, J.C. Watts and others. The idea is also a priority of President Bush.

Entitlement reform is another important area. With the grant from the NCPA, economists at Texas A&M University have developed a model to analyze Social Security and Medicare, and is publishing a series of studies on the future of the two entitlement programs. This work is directed by Texas A&M Professor Tom Saving, who has been appointed a Social Security and Medicare trustee. The NCPA has also established an interactive online Social Security calculator (www.mysocialsecurity.org), that allows visitors to compare their Social Security benefits with returns if they payroll taxes had instead been invested privately.

In the 1980s, the NCPA was the first public policy institute to publish a report card on public schools based on results of student achievement exams, and an NCPA task force made the case for school choice. Subsequently, the NCPA pioneered the concept of education tax credits as one route to school choice. The NCPA and Children First America have published an Education Agenda for the new administration, a book whose contributors include Nobel laureate Milton Friedman, Sen. Jon Kyl and other school choice experts.

The NCPA's Environmental Center works closely with other think tanks to provide common sense alternatives to extreme positions that frequently dominate environmental policy debates. In 1991 the NCPA organized a 76-member task force, representing 64 think tanks and research institutes, to produce *Progressive Environmentalism*, a pro-free enterprise, pro-science, pro-human report on environmental issues. The task force concluded that empowering individuals rather than government bureaucracies offers the greatest promise for a cleaner environment. Later, the NCPA produced *New Environmentalism*, written by Reason Foundation scholar Lynn Scarlett. The study proposes a framework for making the nation's environmental efforts more effective while reducing regulatory burdens. More recent publications include a pathbreaking study that showed the costs of the Kyoto protocol on global climate change would far exceed any benefits.

In 1990 the NCPA's Center for Health Policy Studies created a health care task force with representatives from 40 think tanks and research institutes. The pro-free enterprise policy proposals developed by the task force became the basis for a 1992 book, *Patient Power*, by John Goodman and Gerald Musgrave. More than 300,000 copies of the book were printed and distributed by the Cato Institute, and many credit it as becoming the focal point of opposition to Hillary Clinton's health care reform plan.

A number of bills before Congress promise to protect patients from abuses by HMOs and other managed care plans. Although these bills are portrayed as consumer protection measures, NCPA studies show they would make insurance more costly and increase the number of uninsured Americans. An NCPA proposal to solve the problem of the growing number of Americans without health insurance would provide refundable tax credits for those who purchase their own health insurance. The NCPA has assisted members of Congress to formulate a bipartisan tax credits proposal.

NCPA studies, ideas and experts are quoted frequently in news stories nationwide. Columns written by NCPA experts appear regularly in national publications such as the *Wall Street Journal, Washington Times* and *Investor's Business Daily*. NCPA Policy Chairman Pete du Pont has a weekly column on the *Wall Street Journal's* OpinionJournal.com and another weekly column distributed by the Knight-Ridder Tribune news wire. In addition, his radio commentaries reach 2.2 million listeners across America.

According to Burrelle's, the NCPA was mentioned or quoted in about 15 news articles every day somewhere in the United States in 2000. The advertising dollar equivalent of all print and broadcast coverage was more than $50 million.

The NCPA Internet site (www.ncpa.org) embraces the philosophy of one-stop shopping, linking visitors to the best available information on public policy, including studies produced by think tanks all over the world. Brittanica.com named the NCPA Web site one of the best on the Internet for quality, accuracy of content, presentation and usability.

What Others Say about the NCPA

"...influencing the national debate with studies, reports and seminars."

— TIME

"...steadily thrusting such ideas as 'privatization' of social services into the intellectual marketplace."

— CHRISTIAN SCIENCE MONITOR

"Increasingly influential."

— EVANS AND NOVAK

"The NCPA is unmistakably in the business of selling ideas...(it) markets its products with the sophistication of an IBM."

— INDUSTRY WEEK

ISBN #1-56808-104-9