



September 4, 2001

TRACKS IN CYBERSPACE

Giving the Web a Memory Cost Its Users Privacy

By JOHN SCHWARTZ

The first of three articles.

One day in June 1994, Lou Montulli sat down at his keyboard to fix one of the biggest problems facing the fledgling World Wide Web — and, as so often happens in the world of technology, he created another one.

At that moment in Web history, every visit to a site was like the first, with no automatic way to record that a visitor had dropped by before. Any commercial transaction would have to be handled from start to finish in one visit, and visitors would have to work their way through the same clicks again and again; it was like visiting a store where the shopkeeper had amnesia.

At 24, Mr. Montulli was the ninth employee hired by what would come to be known as Netscape Communications, and was already known as a programmer of exceptional skill. So he quickly came up with an ingenious idea to address the problem and hammered out a five-page document describing the technology that he and co-workers would design to give the Web a memory.

The solution called for each Web site's computer to place a small file on each visitor's machine that would track what the visitor's computer did at that site. Mr. Montulli called his new technology a "persistent client state object," but he had a catchier name in mind, one from earlier days of computing. When machines passed little bits of code back and forth for such purposes as identification, early programmers called the exchanged data "magic cookies." Mr. Montulli would call his invention, a direct descendant, a "cookie."

It was a turning point in the history of computing: at a stroke, cookies changed the Web from a place of discontinuous visits into a rich environment in which to shop, to play — even, for some people, to live. Cookies fundamentally altered the nature of surfing the Web from being a relatively anonymous activity, like wandering the streets of a large city, to the kind of environment where records of one's transactions, movements and even desires could be stored, sorted, mined and sold.

Since then, cookies have become nearly ubiquitous — and that has many people upset. A recent survey by Public Opinion Strategies, a Republican polling organization, found that 67 percent of Americans identify online privacy as a big concern — far more than those who identify fighting crime (55 percent) or building an antimissile shield (22 percent).

Yet while public anger has grown over invasions of privacy both real and imagined, momentum in Washington to restrict the use of cookies and other high-technology tools for monitoring Internet users' activities has slowed.

In Washington, at least 50 privacy-related bills are awaiting consideration, though the current leadership in the House has focused its attention on privacy invasions by government, not by private business. President Bush's recently appointed chairman of the Federal Trade Commission, Timothy J. Muris, is just preparing his first statement on the commission's direction on privacy, to be delivered next month.

Whether willingly, begrudgingly or unknowingly, however, most Web users have already traded a slice of their privacy for the convenience that cookies bring to the Web. Most people accumulate cookies unknowingly; a search on the average Internet user's machine will turn up dozens, or even hundreds, of the small files.

Thanks to cookies, a customer shopping at a site who walks away from the shopping cart before buying can come back later to have the site ask if he wants to complete the order. Cookies also allow sites to show advertisements tied directly to the parts of the site a visitor has seen, so that someone visiting a health-oriented site who reads information about diabetes drugs might see an advertisement for a newly approved medication for the condition.

All these functions can be performed without knowing the name of the visitor because the anonymous, unique identifier included in the cookie is enough. But if a Web site owner can combine that identifier with personal information, say from having visitors register with the site, then the cookie becomes a powerful mechanism for personal tracking.

"Before cookies, the Web was essentially private," said Lawrence Lessig, a professor at Stanford Law School who studies the ways that software code and public policy collide. "After cookies, the Web becomes a space

capable of extraordinary monitoring."

Most business Web sites now use cookies (including the sites of The New York Times Company and most use them responsibly, privacy experts say. But many in business fear that privacy concerns could put a further drag on the hobbled high-technology economy. "The danger to the digital economy's longevity is not from the bursting of the dot-com bubble," said Richard H. Brown, chief executive of the technology giant EDS, in a recent speech.

He cited examples like Toysmart, a company that offered to sell its customer records as part of its bankruptcy settlement — potentially including children's names and addresses. "Those effects are minuscule compared with those inflicted by breaches of trust," Mr. Brown added.

Still, cookies are not going away, said Koen Holtman, a Dutch computer scientist and privacy advocate who has fought to limit the expanding abilities of cookies.

Web users "can't really live with cookies because of user-tracking issues," he said, "but also can't live without them because that would lose them some important functionality or reliability."

Mr. Montulli's first description of cookies can still be found on Netscape's Web site. The document describes how a relatively few bits of text can perform tasks like identifying a visitor, tracking the items he is preparing to buy and setting a date for the cookie to be destroyed. In a whimsical example drawn from Saturday morning cartoons, Mr. Montulli displayed a cookie that might be set on a customer's computer by the fictional Acme Corporation:

Cookie: CUSTOMER=WILEE COYOTE; PARTNUMBER= ROCKETLAUNCHER0001

The document was technically thorough. But one word appears nowhere within it: privacy.

Microsoft Takes Notice

The engineers did build in a few privacy precautions, however. Cookies did not identify the user by name. Instead, each site issues a unique ID number to each visitor's computer. Mr. Montulli said that he also considered and rejected an idea for creating a single ID number that a person's browser would use in all Web explorations; while convenient, it would be, he knew, a privacy nightmare. "We didn't want cookies to be used as a general tracking mechanism," he recalled.

But, Mr. Montulli said, he had also planned for cookies to be a flexible tool — like all Netscape creations. "We were designing the next-generation communications system," he said, and the designers of revolutions don't think small.

"We wanted people to be able to use it for other uses" besides shopping carts, Mr. Montulli said, including "things we hadn't thought about."

By 1995, as Netscape's browser introduced millions of people to the wonders of the Web, another company had taken notice of its success and wanted in on the game. Microsoft aimed at the market for Internet browsers and servers and began a concerted effort that became the focus of the federal antitrust suit against Microsoft.

But when it came to keeping track of online shopping carts, Microsoft decided not to reinvent the wheel, said Michael Wallent, the head of the company's browser efforts. The company's entry in the browser wars, Internet Explorer, largely incorporated Netscape's cookie system as a "no brainer," Mr. Wallent said.

"I don't think anyone ever thought that cookies were anything that could be excluded in the browser and have that browser become a success in the marketplace," he said.

Like Netscape, Microsoft kept its cookies under the table: cookies were designed to be exchanged silently, without alerting the user. With other Web browser functions, like encrypted communication, an icon appears on the computer screen when the technology is in use. Mr. Wallent explained that privacy was not, at the time, a central consideration because the Web "was a very different place."

"While privacy was an issue, it was much less of an issue than you see today," he said.

Although they were not obvious to the average computer user, cookies were quickly noticed within the technology community. Members of the Internet Engineering Task Force, a group that evolved from the time of the Internet's predecessor, the Arpanet, to become the standards-setting body for the ever-evolving worldwide computer network, started in April 1995 to discuss cookies.

Despite Mr. Montulli's prowess, the technology was less than robust. Simon St. Laurent, the author of "Cookies," a technical work, said of Mr. Montulli's original version: "It kind of works, but it's definitely concocted overnight." Discussions began among Internet experts about the kinds of things that Internet engineers fret over, like ways to make the system more secure and reliable. Within the discussion, some were pressing for consideration of privacy issues.

And so, in 1995, a group was formed to come up with proposed standards for cookies and their uses; it was led

by David M. Kristol, a scientist at Bell Laboratories whose outside interests included the intricate interplay of chamber music. He estimated that the job would take a few months.

He worked on it for nearly six years.

Like all such groups, the work was public and carried out largely through online postings and e-mail. Mr. Montulli was an active participant — at least at the beginning. "I remember saying that it was very important that if we made any changes at all to the way things work, that it needed to be a more forward-compatible kind of thing: the old stuff should still work, and people's general idea of cookies will stay the same."

The members of the working group agreed: although they wanted to improve on cookies technology, they realized that whatever recommendations they came up with should work a lot like the current cookies, or the effort would be wasted.

Increasingly, the group became concerned about the ways that cookies might be used to violate consumer privacy. Mr. Holtman, the Dutch computer scientist, issued a warning to the group in December 1995 that would turn out to be prophetic.

Although cookies can only be read by the site that created them or a related site — another of Mr. Montulli's early privacy measures — Mr. Holtman realized that companies could, by agreement, place cookies across a network of related sites, and that those cookies could be used to track users.

"Someone is bound to try this trick," he wrote, "and it will, when discovered, generate a lot of bad publicity for the whole Web."

What Mr. Holtman did not know was that companies were already planning to exploit this wrinkle of the Web. Before long, large Internet advertising companies like DoubleClick ([news/quote](#)) and Engage were displaying ads across thousands of sites, using a common cookie across the network that allowed the company to recognize a visitor wherever he wandered on the Web. The innovation allowed these companies to rotate the ads the user sees from site to site.

DoubleClick's Web site says that it "allows marketers to deliver the right message, to the right person, at the right time." The concern of privacy advocates, however, was that these "third-party cookies" could also be used to build a detailed profile of a Web user's habits.

If a Web surfer visited a large number of sites about AIDS treatment, for example, and if that data were tied to information that identified him — say, registration at one of the sites — an insurance company could, conceivably, collect the cookie data from an ad network and use it in a quiet decision to decline an application for a policy. (Advertising networks insist that they do not sell data for such purposes.)

Third-party cookies were precisely the kind of tracking mechanism Mr. Montulli had tried to prevent through his privacy measures. He describes it today as a surprise — and something of an embarrassment. "That's the one 'gotcha' we had," he recalls with chagrin.

A Hot Media Topic

By 1996, the existence of cookies and third-party cookies was becoming a hot topic in the news media and in online forums; Mr. Montulli and Netscape altered the company's browsers to distinguish cookies coming directly from the site being viewed from third-party cookies and to give consumers some control over them, allowing them to turn off all cookies or just the third-party variety. Microsoft, too, implemented some cookie control tools over time. But by default, browsers were set (and are still set) to accept such cookies automatically unless the user told the software not to — which meant that a great majority of people ended up accepting cookies unknowingly from nearly every site they had visited.

The Internet Engineering Task Force was pursuing a different tack, however, recommending in 1997 that browsers be set to block any cookie that did not come directly from the site being visited.

Mr. Kristol said that the response from the advertising companies, which were by then well established, was: "This is terrible. This will destroy our business." Each argument caused further delay — time in which the advertising companies became more powerful and the market crystallized around the two leading browsers.

Mr. Kristol was not surprised, then, that neither Netscape nor Microsoft took to heart the recommendation that browsers block cookies unless instructed not to. He acknowledged that there was little he could do to persuade companies to adopt the voluntary standards. "There's no Internet police going around knocking on doors and saying, 'Excuse me — the software you're using doesn't follow I.E.T.F. standards.'"

By then, Mr. Montulli said he had drifted away from the process, saying that the working group had, in fact, called for the kinds of technical changes that companies would not comply with. "I was hoping we'd get some kind of incremental improvement" out of the working group, he said — ideas like the cookie control mechanisms he was working into new versions of the browser.

"But what the new standard required," he said, "was that you start over."

To Mr. Montulli, the conflict came down to the differences between pure researchers like Mr. Kristol and

commercial engineers like himself. "The cold reality of the software business is you have to ship something that's good enough and get it out there," he said. "That's the way you ship software, and hopefully make money. If you wait forever trying to make something perfect, you may never ship."

In an article that Mr. Kristol prepared for Communications of the Association for Computing Machinery, the journal of the leading computer science professional organization, he said several factors kept him on his somewhat quixotic task. On one level, "I simply wanted to see the effort through to an appropriate completion," he said. But in his paper, Mr. Kristol — who recently retired from Bell Laboratories — writes, "Feeling I was being bullied" by the industry "made me more determined to persist, and I didn't like to see an attempt to bully the I.E.T.F., either."

If nothing else, the effort raised the visibility of the issues underlying cookies, Mr. Kristol said. Thanks in part to his group's work, he said, companies can't violate consumer privacy, or even appear to, without attracting unwelcome attention.

He cited the controversy that arose when DoubleClick announced in 1999 that it had bought Abacus Direct, a company that maintained a database of the buying habits of 88 million catalog shoppers, and planned to match and merge some of the data that it was collecting online with the offline data from Abacus. The resulting data trove would portray millions of consumers' habits at a level of detail unparalleled in its intimacy.

A Public Outcry

Public outcry over the plan was fierce, and the Federal Trade Commission began an inquiry into the company's practices. DoubleClick abandoned the plan, and the Federal Trade Commission dropped its inquiry. DoubleClick's chief privacy officer, Jules Polonetsky, said, "Companies are learning from the missteps of the past year, and are obligated to bake privacy into the infrastructure of their new products lest they face the wrath of the critics."

Mr. Montulli, now 30, has since gained a measure of fame — not just as the inventor of the cookie, but also as one of People magazine's runners-up for "sexiest man alive" in 1999. He says that he has dialed back from the 120-hour work weeks at Netscape — a punishing life that contributed to the breakup of his marriage to the daughter of Netscape's founder, Jim Clark, in 1997.

He left Netscape in 1998, a millionaire many times over thanks to the company's high-flying stock. He helped to create epinions.com, a site for comparison shopping, but has since left that company as well.

Ask about his latest achievement, and he talks about climbing Mt. Shasta with his girlfriend, Ashley Dearruigunaga — and, at the summit, asking her to marry him. ("At 14,162 feet, I figured she couldn't say no," he said.)

When it comes to cookies, he says that he is satisfied with the way things have worked out. Even though he does not favor the use of third-party cookies, he calls the existence of third-party cookies "the best possible error," because "the only way it could be exploited is by someone who is extremely public, who is extremely large and who has a very long reach" — a company, in other words, that cannot afford a public relations fiasco, he said.

Over time, the views on cookies from privacy advocates have evolved. Richard M. Smith, the chief technology officer for the Privacy Foundation, a think tank in Denver, said that he now believed that most cookies were benign.

"My first reaction was, 'Oh they're terrible!' Over the last year and a half as I've looked at the Internet and how it works, it would be very difficult to have the Internet without them."

[Home](#) | [Back to Technology](#) | [Search](#) | [Help](#)

[Back to Top](#)



[Click Here](#) to Receive 50% Off Home Delivery of The New York Times Newspaper.

Copyright 2001 The New York Times Company | [Privacy Information](#)



SEP 05, 2001

As Big PC Brother Watches, Users Encounter Frustration

By JOHN SCHWARTZ

The second of three articles.

The little silver bags contained a treat — and a taunt: "Do you know where your cookies come from?"

The message was printed on tens of thousands of bags of free chocolate chip cookies that were handed out in six cities last fall as part of an advertising campaign from Earthlink, one of the biggest Internet service providers.

The cookies that Earthlink referred to, of course, were not in the bag but on people's PC's: "cookies" is the term for the small files that Web sites place on visitors' computers to help recall where they have been on the site, to determine which advertisements they see and more.

Although the use of cookies is generally benign, the fact that they can be used for detailed tracking of Web users and their activities has upset many consumers. People shop, chat and play online, and look to the Internet for information on health care, for psychological support and even for love. Meanwhile, the technologies for monitoring and analyzing those activities grow more powerful. But when it comes to protecting privacy online, most consumers still do not even know where to start.

In the campaign, Earthlink compared its privacy policies with those of the industry leader, America Online, and offered its customers tips on how to control cookies.

"Our position is you should be able to understand what's being revealed about you, and you should be able to control it," said Claudia B. Caplan, the company's vice president in charge of brand marketing. Later this year, Ms. Caplan said, the company will also provide software to help customers selectively accept or reject cookies to safeguard their privacy online.

Earthlink said that by the summer it was seeing results: consumer surveys showed that the "unaided recall" of Earthlink's name — that is, the percentage of people who would say "Earthlink" in response to a request to list Internet service providers without prompting — had jumped to 25 percent from 15 percent in the cities where the campaign was used.

"We do believe that privacy was a very, very large component of that," Ms. Caplan said. "We had not seen this kind of movement before the privacy initiative." It remains to be seen, however, whether that will translate into more customers for Earthlink. Privacy, it seems, is something that everybody wants but few want to pay for.

Zero-Knowledge Systems, a Montreal company that offers consumers a full suite of privacy protection tools in its flagship product, Freedom, has also found that getting consumers to pay for privacy can be a struggle. Users can use the company's software to selectively block cookies that Web sites try to put on their machines and can even surf the Internet under pseudonyms, hiding their identities but enjoying the benefits of long-term relationships with online merchants.

Although it has one of the best-of-breed packages for privacy, the company and others like it have not had much luck selling it directly to consumers, said Arabella Hallawell, an analyst with Gartner Inc. ([news/quote](#)) "It became fairly clear that consumers weren't going to buy the kinds of service on offer," she said.

Consumers' headlong dive into the online environment has amplified privacy risks as never before, said Alan Westin, a consultant who has studied privacy and consumer attitudes toward it for more than three decades. "The average person today is engaged in a level of self-disclosure that is truly unparalleled in the history of Western civilization," he said.

Businesses have tried to explain consumers' unwillingness to take steps to protect privacy by saying people do not truly care. WebSide Story, a company that measures Internet traffic on 150,000 sites, reported in April that Web site visitors refuse cookies less than 1 percent of the time — a fact that the company's general counsel and chief privacy officer, Randall K. Broberg, interpreted to mean that "cookies are simply not a big concern among most Internet users."

Advertisement

TECHNO SCOUT.com
Your search ends here

Technology Update

Vision expert creates lamp to reduce eye strain and glare

How to make your car invisible to radar and laser

A floor lamp that spreads sunshine all over a room

Why spend hundreds on a bigger monitor enlarge the one you have

NASA research creates "smart bed" sleep surface

Bring the power of the digital revolution to your fingertips

It's time to put all of your photos onto your computer

[Click for the complete story](#)

Advertisement

But those who study the issue say the real picture is more complex. A snapshot of Web behavior does not show the motivations of the people who click the mouse. That deeper understanding comes through surveys and interviews and not just from Web page statistics, said Donna L. Hoffman, who studies online commerce at Vanderbilt University. "Pages don't talk," she said.

Consumers who do want to reject cookies find the task daunting, said Richard M. Smith, the chief technology officer of the Privacy Foundation, a research center based in Denver. "It's nearly impossible to turn them off," he said.

The hunting and clicking necessary to find and deploy the cookie-control features in most Internet browsers is beyond the ability of most users, Mr. Smith said, and installing add-on software to do the job requires even more effort and expertise. Even when users do set their computers to reject cookies, he said, "what you find is Web sites require them." Even some major Web sites, including The New York Times ([news/quote](#)) on the Web, do not function properly when cookies are rejected.

So what do consumers really want? Despite dozens of surveys of consumer attitudes toward privacy over the years, a nuanced understanding of American attitudes about privacy is only now beginning to emerge. Part of the problem is that no one, in the abstract, is against privacy, so asking whether people favor privacy protection falls under the category that pollsters call "motherhood and apple pie" — questions that almost always generate favorable responses.

Another complicating factor is that even after more than three years of public debate in the news media and the halls of Congress, 56 percent of those surveyed this year on behalf of the Pew Internet and American Life Project did not even know what cookies were — and 34 percent of those who have spent a few years online did not know.

Americans do not speak with one voice on privacy issues, said Mr. Westin, the privacy consultant. He has identified three groups:

First, there are "privacy fundamentalists," who zealously guard their personal information, reject all offers of consumer benefit in return for personal data and tend to be suspicious of efforts by law enforcement to use surveillance technologies like wiretaps.

These are not witless conspiracy theorists and Luddites: many are technology-savvy people like Erin L. Fitch, 23, a receptionist at a law firm in Austin, Tex., who spends plenty of time online but absolutely refuses to shop by computer. She avoids most sites that ask her to register and provide personal information, and says that she does not want to leave herself open to credit card fraud or identity theft because of Web sites with inadequate security.

"I only have one credit card — I don't want to use it," she said, adding (a little defensively) that she was not motivated by fear or worry. "There's nothing to be worried about," she said, "because I'm not putting myself at risk."

On the other end of the spectrum are those Mr. Westin calls the "privacy unconcerned," a group that "for 5 cents off, they'll give you their family history and tell you their vacation plans." These are the people who might have heard the famous comment of Sun Microsystems ([news/quote](#))' chief executive, Scott G. McNealy — "You have zero privacy anyway. Get over it." — and thought it was sound advice.

That is how Beth Wodzinski, a technical writer in Salt Lake City, looks at it. She says she gives out personal data and credit card information online without a second thought about the cookies she may be accumulating or whether someone is looking over her shoulder — largely because she considers herself too small a target for hackers, thieves and snoops.

"A sense of my own irrelevance feeds into it," Ms. Wodzinski, 31, said. "Somehow it all still seems very anonymous and remote. I grew up in a small town in upstate New York where everyone knows everyone else and knows everything about them. That seems much more invasive than a random stranger knowing what my name is."

In the middle of the spectrum are Mr. Westin's "privacy pragmatists," who evaluate risks and benefits, and make decisions case by case. James Twigg, a 70-year-old retiree in Roxana, Ill., keeps up with the technologies that allow Internet activities to be monitored by reading privacy newsletters online; "Reading is a wonderful thing," he says, "but it can almost make you paranoid."

A former computer specialist in the aerospace industry, he has the technical expertise to download and use software that limits the number of cookies his computer accepts and lets him surf the Web anonymously and monitor attempts to enter his computer or to get software to send data out of it. Yet he plays games at the Pogo.com Web site, which requires registration but offers cash prizes, and shops online, "which means I have to trust their privacy policies," he said.

As more people move more of their lives onto the Internet, Mr. Westin explained, longstanding boundaries between the groups have shifted. Until the 1990's, he said, those in the unconcerned group made up about 20 percent of the population, and privacy fundamentalists stood at about 25 percent; the pragmatists occupied the middle 55 percent. But a recent poll by Mr. Westin showed

that the group of unconcerned Americans had shrunk by nearly half, to just 12 percent of the population; the people who shifted, in general, joined the ranks of the pragmatists: not radicalized, but more wary than before.

The largest segment of the population wants to have the ability to make privacy choices, said Harrison M. Rainie, who heads the Pew project. He said that surveys by Pew and others found that consumers "do not want to vest rule-making power in other entities" like government. At the same time, they "feel very comfortable" with government's taking "aggressive enforcement" measures when companies violate their rights, Mr. Rainie said, especially when it comes to abuse of financial information and health data.

Business can lead the way, said Austin Hill, a founder of Zero-Knowledge Systems, the privacy software company in Montreal. He says companies must give consumers relatively painless ways to protect themselves. "We have a huge challenge to make sure that privacy is convenient to users," he said. Zero-Knowledge now focuses on selling its products to other companies so that they can, in turn, offer greater privacy protection to their customers.

Many companies are also exploring ways to serve customers without collecting personal information. Moviephone, for example, provides the names of theaters and show times based solely on the caller's ZIP code. And at the Web site for Palm Inc. ([news/quote](#)), software from a company called Net Perceptions ([news/quote](#)) helps the company make recommendations on Palm gear based on a technology known as collaborative filtering: predicting what a visitor might want based on what other visitors choose, said Nicole Rynee Barnes, the e-business manager for the company.

"We don't require them to log in or give any personal information," she said. Like other merchants in the online world, Palm has learned that violating personal privacy is not worth the damage it does to a company's reputation. "There's huge costs of doing it wrong," she said.

Privacy is a moving target, and notions about it continue to evolve, said Stewart A. Baker, a lawyer in Washington and a consultant on high-technology issues. The initial horror about cookies has undergone a metamorphosis into a more nuanced attitude. "There's always something we consider private and it's something we can keep private," he said. "Those things that we can't keep private we develop a callus over."

"We're going through one of those transitions now," Mr. Baker continued, "but faster."

The important thing, said Frank Torres III of the Washington office of Consumers Union, is that business needs to justify its desire for personal information from consumers. "Giving people a choice doesn't mean they're going to say no," he said. "If you can't convince them, that's a problem from your business perspective. Don't blame it on consumers."

What Americans might really want, said Michigan's attorney general, Jennifer Granholm, is a sense of privacy that is not absolute, but that reassures them. Ms. Granholm, who has mounted aggressive investigations of companies accused of violating consumers' privacy, said that the notion of privacy "can be misconstrued as the right to be left alone."

"What we want is to create a safe place for people to do business and research," she said.

Ms. Granholm said that her thinking had evolved over time, and credits much of the shift to conversations with James E. Tierney, a former Maine attorney general who served on a Federal Trade Commission advisory committee on online privacy and security. Like her, Mr. Tierney said that he had initially been alarmed by the warnings of privacy advocates about the dangers of cookies and intrusion. But, he said, he had come to realize that this was not a nation of Greta Garbos and Theodore J. Kaczynskis.

"Privacy is not about being left alone," Mr. Tierney said; citizens should be able to feel that the personal data that they entrust to others is protected. "It's about safety."



September 6, 2001

TRACKS IN CYBERSPACE

Government Is Wary of Tackling Online Privacy

By JOHN SCHWARTZ

The last of three articles.

Mozelle W. Thompson took a stroll last summer through the Silicon Alley Street Fair, a celebration of New York City's dot-coms back when they had something to celebrate. His T-shirt and shorts belied his high office as a member of the Federal Trade Commission, the federal agency that has taken the lead in consumer privacy protection online. He met the chief executive of a high-technology company that gathers personal data on Internet users, a man who was, Mr. Thompson said, "treating people as data instead of treating people as people."

Mr. Thompson asked the executive whether he worried that regulators might some day crack down on his business practices. Mr. Thompson's eyes went wide as he recalled the man's answer: "I'm going to do as much as I can, as fast as I can — until somebody stops me." As for the Federal Trade Commission, Mr. Thompson said, "He didn't know me, and he didn't know us."

"But I assured him he would."

Since then, the world has changed, and not just for the dot-coms. Momentum has dissipated in Washington for new laws and regulations that might restrict the use of cookies and other high-technology tools by businesses to monitor Internet users' activities. Some lawmakers say that the politics of privacy is so touchy and complex that a deliberate approach is best — but there is growing agreement that some kind of government action will eventually have to emerge.

Mr. Thompson still serves on the Federal Trade Commission, but Robert Pitofsky, the chairman who led many of the commission's privacy initiatives, has been replaced by Timothy J. Muris, a former trade official in the Reagan administration who has said he is still studying the privacy issue. President Bill Clinton, who appointed Mr. Pitofsky and Mr. Thompson, has been replaced by President Bush, whose executive branch team has been less than enthusiastic about expanding regulatory authority over businesses.

Movement toward legislation restricting invasions of consumer privacy by business has slowed in Congress, as well: although the chairman of the Senate Commerce, Science and Transportation Committee, Ernest F. Hollings, Democrat of South Carolina, has a strong interest in privacy, the Senate is currently bogged down in the appropriations process and other issues. The leadership of the House has called for the debate to be refocused on the misdeeds of the government rather than those of companies.

"Let's see to it that the government is handling privacy mandates properly before we start mandating privacy rules for the private sector," said Richard Armye, the House majority leader, in an interview, citing such examples as government Web sites that store personal information, the F.B.I. Internet wiretap system known as Carnivore and cameras that photograph motorists who run red lights.

Some in Congress say that the loss of momentum to regulate technologies like cookies can be attributed to a more subtle understanding of the interplay of privacy and technology. Senator Patrick Leahy, Democrat of Vermont who has long been concerned about privacy issues, said that he and other lawmakers had realized that simple responses to privacy fears, like sharply restricting the use of cookies, would do more harm than good.

"Cookies have gotten bad press as a surveillance tool, but they also make Web site visits faster and online transactions more hassle-free," Senator Leahy said in an e-mail response to a reporter's questions. "These are important functions for Internet users, and any regulation of the use of cookies must be sufficiently nuanced to ensure that we do not throw the proverbial baby out with the bath."

Little wonder that privacy has emerged as one of the thorniest issues for policy makers, said Peter Swire, the former privacy counselor to Mr. Clinton. The issues are complex, and they pit passionate public opinion against equally powerful business interests. "The strongest impetus for action and the strongest resistance to action have come together on the Internet privacy debate," he said.

Federal efforts to regulate privacy took off within the Federal Trade Commission in 1995, recalled a former staff member, David Medine, when "we realized the Internet collects a lot of information about people cheaply, efficiently and sometimes in unprecedented ways — like what you looked at as opposed to what you bought, which in a store would never be collected." After working with industry to develop self-regulation efforts, the commission asked Congress last year to expand its legal authority to regulate privacy efforts when self-regulation fails.

That call for Congressional action has gone unheeded. But several laws have been passed in recent years in the areas of highest concern to voters. Financial institutions must now send out notices describing their privacy policies under the terms of the Gramm-Leach-Bliley Act of 1999, and new health care privacy regulations are coming into effect because of the Health Insurance Portability and Accountability Act of 1996. The privacy of children has been shored up because of restrictions on data collection under the Children's Online Privacy Protection Act of 1998.

These laws, however, leave some elements of privacy protected and others utterly exposed. Privacy advocates see the job of filling in the holes as their challenge; business sees it as a threat.

At least 50 privacy-related bills are awaiting consideration this year, many of them new versions of bills introduced in the last session of Congress. No matter how varied the legislation, proposals generally come down to a few crucial requirements and distinctions. Most require that consumers be notified of the ways companies collect data and the use they will put that information to and require that companies give consumers the ability to say no to such collection.

The crucial distinction is the way consumers can say no: by "opting in" or "opting out." For example, a recent Senate bill co-sponsored by John McCain, Republican of Arizona, and John Kerry, Democrat of Massachusetts, would require companies to give consumers the right not to have their personal information collected via cookies or other technologies.

The bill would set a standard, but consumers must make the effort to "opt out" of data collection, which means most will, through inertia or ignorance, stay on the rolls. Privacy advocates generally favor a higher "opt in" standard, which would prohibit collection of information without explicit permission from consumers — an approach taken by another bill introduced by Senator Hollings in 2000; a version will be reintroduced this fall.

Whatever route lawmakers choose, said Priscilla M. Regan, an associate professor of government at George Mason University in Virginia, privacy is exactly the kind of area in which government action can lead to a benefit to citizens. "The costs to the individual are just enormously high in terms of time and energy and an individual's attention to detail," she said.

Even though most people do not take action to preserve their privacy, the rights of those who do want protection have to be upheld, said Marc Rotenberg, the executive director of the Electronic Privacy Information Center in Washington. "The right of privacy is not simply a ratification of a majority practice," he said. He compared safeguarding personal data to the American system of food safety, which gives consumers control over what they purchase but leaves a role for government in protection beyond the capabilities of individuals. "Not many of us have a fully equipped U.S.D.A. lab in our basement that we can run two pounds of chuck through at night when we get back from the supermarket."

Representative Armev, Republican of Texas, disagrees. He sent a letter to his colleagues in April warning them against taking any action in the current legislative session because, in his view, government can only make a mess of privacy. "Congress is an inexperienced and amateur mechanic trying to tinker with the supercharged, high-tech engine of our economy," he said. "We need to be careful not to let our good intentions get in the way of common sense."

Lawmakers like Mr. Armev are bolstered in their efforts to slow the march of legislation by a flood of new studies and surveys sponsored by high-technology companies, questioning consumer attitudes about privacy and giving multibillion-dollar estimates of the costs of complying with such laws.

Thus a study by Robert Hahn of the American Enterprise Institute, a conservative research center in Washington, concludes that complying with privacy legislation proposals would cost companies a staggering \$30 billion. Such figures help industry spokesmen like Jonathan Zuck of the Association for Competitive Technology, which paid for the Hahn study, to argue that "the costs associated with regulation appear to be higher than the benefits achieved by regulation."

Robert Gellman, a privacy consultant in Washington, calls the new crop of studies "put-up jobs" with inflated estimates. He ridicules the private sector's opposition to legislation, saying, "The industry is willing to spend millions for studies, but nothing for privacy."

Mr. Hahn defends his study, saying that if anything, the estimates are conservative. He has also drawn attention recently with a study suggesting that the benefits of lowering arsenic levels in drinking water would not justify the costs. "I made my best assessment," he said.

The price of inaction, however, could be precisely the kind of overreaction that Senator Leahy warns against, legislative experts say. Highly visible violations of privacy have tended to generate specific — and, often, narrow — legal responses, leading to a patchwork of legal remedies. Lawmakers were quick to pass legislation making it illegal to release video-rental records after a list of rentals by Robert Bork, a Supreme Court nominee, was leaked, for example. And Florida moved to seal autopsy records after a fight over publishing the death photos of the Nascar racer Dale Earnhardt.

Quick-fix legislation rarely fixes anything but lawmakers' standing in the polls, said Stewart A. Baker, an lawyer in Washington who consults with companies on technology policy issues. Legislation is "often just a set of palliatives" that is unlikely to do much for consumers, he said.

"All that allows you to do," he added, "is that you can say, 'Well, we passed a law.'"

The Internet has presented a never-ending set of complaints: consumers and privacy advocates raged when the online advertising giant Doubleclick announced in 1999 its intention to combine personal data identifying many visitors to its affiliated Web sites with a large database of catalog shopping information that it acquired in a merger with a company called Abacus Direct. Another company, Toysmart, raised consumer fears in 2000 when it tried to sell its user records to raise money in bankruptcy proceedings; the company's data included personal information on children. But privacy experts say they worry about the dangers of government overreaction to such episodes. Public concern over cookies, for example, has already led to some results that even the most ardent privacy advocates say have been bizarre. Last year, the Clinton administration, for example, prohibited the use of cookies on any federal Web site without permission from the head of the site's agency — a decree that ignored the usefulness of cookies in helping visitors to a Web site remember where they have been and to ease their navigation.

"I think the government has swung too far," said Mr. Rotenberg, the privacy advocate. "Everything is without any historical dimension. It's, 'Help! There's a cookie on my computer! Someone get in here!'"

That is why Mr. Swire says, in fact, that the current lull might be helpful, so long as a full-bodied debate on privacy continues. "We should learn from our medical and financial privacy experience," he said, "and now we're getting a chance to do so." The stakes, Mr. Swire added, are huge: "It's not just human rights, and it's not just burden on industry. It's how to get the rules and the systems right for the information age."

One way or another, Mr. Rotenberg said, new privacy laws will emerge. "I don't think that Mr. Armev and the Republicans and the army of lobbyists that surround our president can make this issue go away." He suggested that the crisis- to-crisis collage of laws should be reshaped into "a legal framework that sets out how these technologies are used."

Business itself could lead the charge for legislation, said Mr. Gellman, the privacy consultant — especially if the federal lawmakers are reluctant to act and states take up the issue. That could lead to a patchwork of inconsistent and even conflicting laws in many states. That, in turn, could bring companies back to Washington to lobby for a federal privacy law that would set a national standard and nullify, or pre-empt, state efforts. "You know who really wants privacy legislation — and won't admit it — is industry, because they want pre-emption," he said.

Sensing the troubles to come, Mr. Thompson of the Federal Trade Commission issued a warning earlier this year to executives at a high- technology conference in New York: Without the legal protection that comes with regulatory structure, he said, horror stories will accumulate and damage will be done and "your stock valuation will continue to sink into the sunset."

The companies, he said, will have to prove to consumers that giving up privacy is a trade — something companies can prove will repay them in convenience and services, without the nasty surprises of seeing the information leak out into the broader world.

"The worst thing we could do to you," he said, "is to do nothing."