

# Keeping Big Brother From Watching You: Privacy in the Internet Age

A CITIZENS AGAINST GOVERNMENT WASTE SPECIAL REPORT

---

## Introduction

In his classic novel *1984*, George Orwell depicts the nation of Oceania ruled by Big Brother—government in control of all aspects of life through constant video surveillance and the control over peoples' beliefs and opinions. The Thought Police, charged with maintaining order and love of Big Brother, keeps careful watch over—and control of—the citizenry. The vain struggles of Orwell's protagonist to win a small slice of liberty serve as a stark allegory of totalitarianism's threat at the dawn of the Cold War.

While America today clearly does not resemble Oceania, the advent of the Information Age raises old concerns about protecting personal privacy and proprietary information, including medical and financial data, from the government, private companies, and other individuals. Information on one's personal habits is increasingly gathered through myriad transactions, including credit card charges, cell phone calls, and check card purchases at the local grocery store. While these activities are generally financially secure, data from such New Economy tools can be used to keep track of people's personal preferences. In today's world, Orwell's concerns can shed light on the collection of personal medical or financial information by federal government agencies, and the sharing of that information with other agencies to be used against the purpose it was collected for.

The difference between privacy in the public and private sector is clear. In the public sector, the citizen has no choice but to provide the federal government with legally required information in the form of tax returns, a Social Security number, student loan information and other data to the federal government. It is precisely because of this authority that the government has the highest legal and moral obligation to ensure that this information is protected, especially as citizens have little recourse to compensation if it is used incorrectly.

In the private sector and on the Internet, however, the citizen has numerous options to withhold information—the ability to disable cookies, use P3P technology built into browsers, and examine a site's privacy policy and move on if the provisions are unsatisfactory, just as one would walk out of a store with poor service or quality in the offline world. Additionally, if users feel the site is not complying with its posted privacy policy, just as they do when a business promises and fails to keep personal information private, while causing harm, they have recourse to legal action.<sup>1</sup> Furthermore, since

---

<sup>1</sup> Eugene Volokh, Law Professor, University of California-Los Angeles, "Warning, Congress! Look Before you Leap into Internet Privacy Thicket,"

<http://www.techcentralstation.com/NewsDesk.asp?FormMode=PolicyTracksArticles&ID=11>, p. 2.

April 2000, the Federal Trade Commission (FTC) has had the right to bring enforcement actions and impose civil penalties for violations of privacy law.<sup>2</sup>

The key to privacy is choice in providing information—it can be controlled in the private sector, but in the government it's compelled by law.

---

## Privacy and the Federal Government

Today, the federal government collects more personal, medical and financial information about people and their families than any other entity. It is unlikely that many Americans are aware of the extensive information gathered about them and controlled by the federal government. Your name, address, race, income, student records, medical history and other data is on magnetic tape or other media all over Washington, D.C. Here are just a few examples:

- The Commerce Department—Individual and Household Statistical Surveys, which include an individual's name, age, birth date/place, sex, race, home/business phone, address, family size and composition, patterns of product use, drug sensitivity data, medical/dental/physical history, and such other information as is necessary. Other lists include Minority-Owned Business Survey Records and Users of the Public Room of the Patent & Trademark Office.
- The Department of Education—National Student Loan Data System and a Registry of Deaf-Blind Children/Regional-National.
- The Department of Energy—Records of Alien Visits, Counterintelligence Investigative records, records of power sales to individuals, as well as Human Radiation Experiments records.
- The Federal Bureau of Investigation—FBI Central Records System, Alien Address reports, the Witness Security Files Information System, and parole records.
- The Department of Health and Human Services—massive quantities of medical records in the National Claims History Billing and Collection Master Record System and the Person-Level Medicaid Data System.
- The Department of Housing and Urban Development (HUD)—Single Family Research Files, mortgage files, Income Certification Evaluation Data Files and Tenant Eligibility Verification Files.
- Department of the Interior—Individual Indian Monies database, Indian Student Records and lists of Foreign Visitors and Observers.
- The Department of Justice (DOJ)—Inmate Physical and Mental Health Records System and other information related to prisoners, as well as an Information File on Individuals

---

<sup>2</sup> "Is Privacy a Thing of the Past?" <http://netprivacypower.org/privacy/index.htm>.

and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities. DOJ also holds Registration and Propaganda Files under the Foreign Agents Act of 1938, and tracks citizen's purchases under the DEA Essential Chemical Reporting System. The Department is also home to the Automated Intelligence Records System known as Pathfinder.

- The Department of Labor—Applicant Race and National Origin System, Injury Compensation System, National Longitudinal Survey of Youth and a Workers Compensation database.
- The Social Security Administration—Information on the lifetime earnings of all Americans as well as certain information relating to insurance, health care and census data. Databases include the Matches of Internal Revenue Service and Social Security Administration Data with Census Survey Data, the Kentucky Birth Records System, and databases on Cuban and Indochinese refugees.
- The Department of the Treasury—The FinCEN Database, which contains millions of reports on the banking activities of individually named citizens, as well as a database of relocated witnesses. It also has files of derogatory information about which no action has been taken, Electronic Surveillance Files, and the Office of Thrift Supervision's Confidential Individual Information System. Within the IRS, there is now a National Database of New Hires, which holds records of the income of every working American.<sup>3</sup>

The National Database of New Hires was established in 1996, and requires that all employers report identifying information about all new employees for inclusion in the database. This database is being used to enforce state child support orders. New employees must be entered into the database whether they have violated a child support order or not, whether they have children or not. The IRS, the Social Security Administration and the Justice Department will also all be able to access the database.<sup>4</sup>

Lately, the growth in government databases has created some disturbing, almost Orwellian trends, as information from one federal agency has been freely given to another to create a catch-all umbrella database, capable of building up a complete profile of an individual from records faithfully supplied to the federal government in trust by the citizen. According to a recent report released by the privacy think tank Privacilla,<sup>5</sup> there has been an alarming increase in the amount of personal information that federal agencies collect and share with one another, including 47 separate instances where federal government agencies announced their intent to exchange personal data and combine it into their own databases.

An April 2001 report by the Senate Committee on Governmental Affairs shows why this could be a dangerous trend. The committee found that people who log onto dozens of federal government Web sites can be unknowingly tracked, despite a privacy policy

---

<sup>3</sup> Solveig Singleton, Director of Information Studies, Cato Institute, Testimony Before the House Subcommittee on Government Management, Information, and Technology, Washington, D.C., Sept. 11, 2000, p. 3.

<sup>4</sup> Solveig Singleton, "How Big Brother Began," Cato Institute, Washington, D.C., Nov. 25, 1997, p. 1.

<sup>5</sup>"Privacy and Federal Agencies: Government Exchange and Merger of Citizen's Personal Information is Systematic and Routine," <http://www.privacilla.org>, March 21, 2001.

forbidding it.<sup>6</sup> The report, culled from audits of 16 agencies, found 64 federal Web sites used files that allow them to track the browsing and buying habits of Internet users. These were not random examinations. Jupiter Media Matrix, a company that tracks Internet usage, estimated 3.5 million visitors clicked on the Education Department's Web pages in March and 2.2 million visited NASA sites.

In total, seven federal agencies have software that collected unauthorized information from visitors, including the Transportation Department's 23 Web sites, the General Services Administration's 15 sites and the Energy Department's 11 sites.<sup>7</sup> Federal agencies are blatantly ignoring the law stating that this kind of software can only be used when there is a compelling need, and even in these instances, Web sites must explicitly inform Internet users about the practice.

This report brings to light one of Orwell's worst fears—not only are government agencies sharing private, personal information about individual citizens and failing to inform them, but they are also overstepping checks and balances designed to prevent such abuses from occurring. Governmental Affairs Committee Chairman Fred Thompson (R-Tenn.) emphasized that the government was technologically challenged when he said that “the Administration is not enforcing the laws that Congress passed” and that the federal government's underlying infrastructure is “riddled with vulnerabilities which represent severe security flaws and risks to our national security, public safety, and personal privacy.”<sup>8</sup>

---

## Security ... What Security?

The Senate Committee report represents the tip of the iceberg when describing the government's abysmal track record of protecting sensitive information. In a survey conducted in March 2001 by the FBI and the Computer Security Institute, 85 percent of the companies and governmental agencies surveyed indicated that they had detected computer security breaches in the previous twelve months.<sup>9</sup> Identity theft alone has increased year after year.

Without proper safeguards, the merging of government databases poses an enormous risk, making it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against computer networks and systems. The General Accounting Office (GAO) cited several serious computer security incidents that have occurred since early 1998, resulting in damage and disruption to agency operations. As a result of these weaknesses, computer systems and the operations

---

<sup>6</sup> *Major Management Challenges Facing Federal Departments and Agencies*, Senate Governmental Affairs Committee, Washington, D.C., April 2001, p. 2.

<sup>7</sup> “Federal Web Sites can Track Visitors,” *The Washington Times*, April 17, 2001.

<sup>8</sup> <http://www.senate.gov/~thompson/compsec.html>, Accessed April 27, 2001.

<sup>9</sup> Robert F. Dacey, Director, Information Security Issues, General Accounting Office, Testimony before the House Energy and Commerce Subcommittee on Oversight and Investigations, Washington, D.C., April 5, 2001, p. 2.

that rely on the systems were highly vulnerable to tampering, disruption, and misuse from both internal and external sources.<sup>10</sup>

Not only does the federal government have inadequate protection for this highly sensitive information, they are guilty of a greater hypocrisy: as consideration is being given to regulating online privacy, federal agencies don't even follow their own rules on the privacy of shared personal and financial information. GAO testified in September 2000 that both the FTC and the government as a whole failed to live up to the privacy standards that the FTC asked Congress to impose on the private sector.<sup>11</sup>

Moreover, the House Government Reform Subcommittee on Government Management, Information and Technology found the federal government's computer security so lax it merited a D- grade overall.<sup>12</sup> The best agencies were the Social Security Administration and the National Science Foundation with Bs, but more than one quarter of all agencies received an F, including the Departments of Labor, Justice, Health and Human Services, and the Small Business Administration. The most disturbing grade was received by Department of Defense, whose computers carry some of the nation's most sensitive secrets, and which earned a D-plus for its computer security program.

Subcommittee chairman Steve Horn (R-Calif.) called the report "dismal" and underlined that there is "no room for complacency, for the stakes are simply too high."<sup>13</sup> House Majority Leader Richard Armey (R-Texas) concurred with this sentiment in April 2001 when he said that "there are plenty of things we can do to improve the way the federal government uses personal information—both in the bureaucracy and in Congress. We should clean our own house before dictating solutions to others."<sup>14</sup>

In the name of transparent and even more efficient government, a great number of federal databases are kept online—a laudable goal that can make life easier for the average American. However, improved access can easily be abused if the security of these files is not held to the highest standards.

---

## Agency Abuses and Failures

One example of a federal agency which has breached its own guidelines on privacy time and again is the Internal Revenue Service (IRS)—an agency one would assume to have the most stringent security controls considering the type of information it handles. In 1995 for example, more than 500 IRS agents were caught illegally snooping through the tax records of thousands of Americans, including personal friends and celebrities. Only five were fired for that gross misconduct.<sup>15</sup>

---

<sup>10</sup> *Ibid.*, p. 8.

<sup>11</sup> Joel C. Willemssen, Director, Civil Agencies Information Systems, Accounting and Information Management Division, Testimony before the House Government Reform Subcommittee on Government Management, Information and Technology, Washington, D.C., Sept. 11, 2000.

<sup>12</sup> <http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911reportcard.htm>, Accessed April 26, 2001.

<sup>13</sup> <http://www.house.gov/reform/gmit/hearings/2000hearings/000911.../000911sh.ht>, Accessed April 26, 2001.

<sup>14</sup> Richard K. Armey, U.S. House Majority Leader, April 2001.

<sup>15</sup> Lucas Mast, "The Feds and Your Privacy," The Cato Institute, Washington, D.C., Sept. 27, 2000.

In February 2001, GAO issued a report concerning information security in the IRS.<sup>16</sup> GAO discovered that during the 2000 tax filing season, the IRS did not adequately secure access to its electronic filing systems or the electronically transmitted tax return data these systems contained. The auditors found that no encryption was used to protect tax return data on e-file systems—an eye-popping lapse in security—and even demonstrated that they could access a key electronic filing system using a common handheld computer.<sup>17</sup>

The IRS had failed to construct firewalls and similar perimeter defenses to protect these files, giving the average hacker easy access to high level sensitive data. While the IRS stated it did not have evidence that any intrusions occurred or that intruders accessed or modified taxpayer data on its e-file systems, the agency also did not have adequate procedures to detect such intrusions at the time.<sup>18</sup> The IRS wasn't even aware of GAO's testing of its system vulnerabilities.<sup>19</sup>

In addition, GAO found that the IRS did not implement adequate password management and that IRS personnel often “turned off” network control devices in order to speed up the processing of electronic tax returns. The agency also processed electronic tax returns and paid refunds without a taxpayer's signature—the practice that certifies the return is true, correct, and complete to the best of the taxpayer's knowledge. This means that the IRS paid refunds of about \$2.1 billion on electronic tax returns that were not authenticated by taxpayers as of August 24, 2000.

The failure to catch such mistakes and the lack of modernization generally within the IRS has cost taxpayers millions of dollars. For example, the IRS's Cyberfile project, designed to enable taxpayers to file returns from home, cost taxpayers \$17 million—and it never even worked. The agency also spent \$251 million before canceling as "worthless" its Data Processing System, which was designed to scan and store tax forms.<sup>20</sup> The IRS's penchant for waste and abuse is well-documented and is, according to GAO, related to lack of expertise, lack of accountability at both the IRS and the Treasury Department, and lack of continuity among senior IRS officials.

Electronic returns provide some of the most damning evidence against the IRS, especially as the IRS asserts in promotional material that the security and privacy of tax return data filed electronically is “assured”.<sup>21</sup> What the IRS did not disclose was that taxpayer information was not encrypted as promised, but sent in clear text, so that the transmission could be viewed, modified or copied unbeknownst to the sender. According to GAO, the IRS also approved individuals as e-file trading partners who possessed unpaid tax liabilities, filed late tax returns, filed false tax returns, or were assessed Trust Fund Recovery penalties.<sup>22</sup>

---

<sup>16</sup> *Information Security: IRS Electronic Filing Systems*, GAO-01-306, Feb., 2001.

<sup>17</sup> *Ibid.*, p. 2.

<sup>18</sup> *Idem.*

<sup>19</sup> *Ibid.*, p. 11.

<sup>20</sup> Rob Wells, “Bidders in First IRS Fiasco Back for More, Agency Blames Itself, But Study Finds Others Culpable,” *Rocky Mountain News*, July 5, 1998, p. 4A.

<sup>21</sup> *Information Security: IRS Electronic Filing Systems*, GAO-01-306. Feb. 2001, p. 13.

<sup>22</sup> *Ibid.*, p. 14.

While the IRS is one of the worst offenders, most other agencies are also technologically challenged. In its April 2001 testimony before the House Energy and Commerce Subcommittee on Oversight and Investigations, GAO summarized the information security audits that had been performed since July 1999 at 24 major departments and agencies.<sup>23</sup> A few examples of weaknesses in federal government computer systems demonstrate the danger not only to individual privacy, but also to national security:

- A hacker group called “PoizonB0x” defaced numerous government Web sites, including those of the Department of Transportation, the National Science Foundation, the National Oceanic and Atmospheric Administration, the General Services Administration, and the Office of Science and Technology Policy.<sup>24</sup>
- In February 2001, the Department of Health and Human Services’ (HHS) inspector general reported “serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.”<sup>25</sup> The greatest weaknesses were at the Health Care Financing Administration, which in fiscal year 2000, processed more than \$200 billion in Medicare expenditures.<sup>26</sup>
- In June 1998, the Environmental Protection Agency (EPA) was notified that one of its computers was used by a remote intruder to gain unauthorized access to a state university’s computers. Although software updates were available to correct the vulnerability, EPA had failed to install them.<sup>27</sup>
- In June 1999, a similar failure to update software over a three year period allowed an intruder penetrate an Internet Web server at EPA’s National Computer Center. The hacker exploited a control weakness specifically identified by EPA about three years earlier during a previous penetration of a different system.<sup>28</sup>
- In September 1999, an individual who no longer had an official affiliation with EPA gained access to an agency computer and altered the computer’s access controls, thereby blocking authorized EPA employees from accessing files. In simple terms, EPA failed to remove the individual’s access codes to its computers after he stopped working there.<sup>29</sup>
- At one agency, 11 procurement staff members possessed system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 were allowed to edit vendor files, allowing them possibly to append fictitious vendors to the file. GAO identified 60 purchases, totaling about \$300,000, that were requested, approved, and receipt-recorded by the same individual in fiscal year 1999.<sup>30</sup>

---

<sup>23</sup> Ibid., p. 2.

<sup>24</sup> Ibid., p. 24.

<sup>25</sup> Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000, A-17-00-00014, Feb. 26, 2001.

<sup>26</sup> Dacey Testimony, pp. 6-7.

<sup>27</sup> Ibid., p. 7.

<sup>28</sup> Ibid., p. 8.

<sup>29</sup> Idem.

<sup>30</sup> Ibid., p. 14.

GAO called these lapses in information security “a widespread federal problem with potentially devastating consequences.”<sup>31</sup> Weaknesses in the policies, procedures, and technical controls that apply to an agency’s information systems and their operation “placed a broad range of critical operations and assets at risk for fraud, misuse and disruption. In addition, they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.”<sup>32</sup>

These lapses in security have been so pervasive for so long that since 1997 GAO has placed information security on its high-risk list.<sup>33</sup>

The Bush Administration has recognized that these failures need to be remedied. As part of this effort, the Commerce Department has announced a new position to protect its sensitive information and respond to questions citizens might have relating to privacy and the federal government. The President’s fiscal 2002 budget contains \$100 million over three years for an interagency electronic government (e-gov) initiative. In addition, the budget calls for increased access to information and services through the Internet, which would include “transactions with the public along secure Web-enabled systems that use portals to link common applications and protect privacy.”<sup>34</sup> The administration’s goal is laudable as long as agencies take their responsibilities to protect personal data seriously and invest sufficient resources to prevent abuses.

---

## The Threat of Government Regulation of Privacy

During the last few years, executive agencies and Congress have been making ever louder noises about privacy laws and regulations for the private sector, despite the hypocrisy of the federal government’s own failed attempts to protect sensitive information. In May 2000, a majority of the Federal Trade Commission (FTC) agreed that legislation would be needed to “supplement self-regulatory efforts and guarantee basic consumer protections.” FTC Commissioner Orson Swindle dissented vehemently from this decision, calling it an “unwarranted reversal” of previous FTC support for self-regulation, concluding that legislation could impose “costs or other unintended consequences that could severely stifle the thriving New Economy.”<sup>35</sup>

In addition to the FTC’s foray into privacy regulation, the National Association of Attorneys General (NAAG) dedicated its summer 2000 meeting to the issue of privacy. NAAG decided upon a set of “Privacy Principles” that it would offer to Congress as a foundation for federal privacy legislation.<sup>36</sup> The principles themselves seem innocent enough, consisting of notice, choice, access, security, and enforcement/redress.

---

<sup>31</sup> *Ibid.*, p. 3.

<sup>32</sup> *Idem.*

<sup>33</sup> *Ibid.*, p. 4.

<sup>34</sup> *A Blueprint for New Beginnings, A Responsible Budget for America’s Priorities*, Fiscal Year 2002, p. 179.

<sup>35</sup> “Federal Trade Commission Recommends Congressional Action to Protect Consumer Privacy Online,” <http://www.ftc.gov/opa/2000/05/privacy2k.htm>, May 22, 2000, p. 2.

<sup>36</sup> <http://www.naag.org/>, Accessed April 27 2001.

However, when read in detail they seem severely suppressive in their monitoring of the online industry. Under “Notice,” for example, the user must be aware of the identity of the entity collecting the data, how it will be used, its potential recipients, whether the requested data is given voluntarily or not, and the consequences of a refusal to provide the requested information. This does not give the company collecting the data much flexibility over how it will be used, a huge disadvantage in areas such as marketing.

Several industry associations have expressed concern over both the NAAG principles and congressional activity. The Association for Competitive Technology was “particularly troubled with the notion that comprehensive privacy legislation is necessary.”<sup>37</sup> The Association of National Advertisers agreed, stating that “imposing cumbersome or overly restrictive rules in the electronic marketplace could destroy the interactive value of the Internet.”<sup>38</sup> Comments from the Information Technology Industry Association expressed concern that by “encouraging precipitous and unnecessary regulatory steps intended to enhance privacy, the NAAG Principles may actually give consumers fewer choices and, as technology changes, less privacy.”<sup>39</sup> FTC Commissioner Leary also stated that a “focus only on online privacy issues could ultimately have a detrimental impact on the growth of online commerce” because “online companies will be placed at a competitive disadvantage relative to their offline counterparts.”<sup>40</sup>

---

## Legislative Initiatives

To date, more than forty bills related to privacy have been introduced in the 107<sup>th</sup> Congress related to medical data, marketing practices, and financial information.<sup>41</sup> Three hearings have been held on the subject through April 2001.

Among the most sweeping proposals is H.R. 89, the “Online Privacy Protection Act of 2001,” sponsored by Rep. Rodney Frelinghuysen (R-N.J.). The legislation requires Web site operators to provide a process for individuals to consent to or limit the disclosure of personal information collected online. It also allows the states to enforce provisions of the act by bringing action on behalf of residents.

Rep. Anna Eshoo (D-Calif.) is the sponsor of H.R. 237, the Consumer Internet Privacy Enhancement Act. The legislation would make it unlawful for a commercial Web site operator to collect personally identifiable information online from a user, unless the operator provides notice and an opportunity to limit the use of the information or disclosure to third parties. The notice would have to include the identities of the Web site and any third party collecting the data, with a link to the third party Web site.<sup>42</sup>

Other measures that have been proposed in the 107<sup>th</sup> Congress include the establishment of a Privacy Commission (H.R. 583), which would report on issues relating to protection

---

<sup>37</sup> <http://www.privacyalliance.org/naag/>, Accessed March 21, 2001.

<sup>38</sup> Idem.

<sup>39</sup> Idem.

<sup>40</sup> Idem.

<sup>41</sup> <http://www.privacy.org/article.php?sid=714&mode=thread&order=0&thold=0>, p. 1.

<sup>42</sup> J. Mark Huffmann, “Feature: Web Privacy Returns to Congress,” UPI Science News, Jan. 26, 2001, p. 2.

of individual privacy and the appropriate balance to be achieved between protecting such privacy and allowing appropriate uses of information. H.R. 347, the Privacy and Disclosure Act, requires the FTC to prescribe regulations to protect the privacy of personal information collected from and about individuals on the Internet and to provide greater individual control over the collection and use of that information.

What often goes unrealized is the cost of such federal intervention. A May 2001 study concluded that U.S. companies doing business online would have to pay \$9 billion to \$36 billion to modify their Web sites to comply with proposed privacy laws. Moreover, small businesses would be hit hardest, since they own the great majority of working Web sites. The study concluded that further regulation of online privacy is not necessary because the direct costs of compliance could be substantial, the benefits have yet to be quantified, and the marketplace is responding to consumer demands.<sup>43</sup>

---

## Legislating is Slow, Cumbersome, and Inflexible

A major drawback of government action on privacy is the inability of the government to keep up with technology. Changes in the high tech marketplace occur far faster than politicians can act. Passing legislation takes time, and policies applicable today would quickly become obsolete.

Such mandates also limit consumer choice and personal preferences, a key benefit of online use. Software releases begin at 1.0 and can go up as far as the technology permits. These new and improved versions meet consumer demand, yet legislation has no built-in mechanism to do this. There is no expectation of future versions of legislation as there is no expectation that laws will be changed quickly, or ever. Companies can quickly change their policies without legislation. Any regulatory scheme would not be able to respond to a vibrant and competitive marketplace the same way that businesses can.

In addition to the lengthy legislative process, the regulations necessary to implement a law take months or years and Congressional oversight is usually abysmal. Promulgation of regulations also creates interest groups with a desire to maintain that law. Government regulations are also extremely inflexible. Once a major law is passed, it tends to establish a regulatory framework that lasts for a long time. It will “freeze technology,” destroying incentives for innovation, since innovation will not satisfy the government’s requirements.<sup>44</sup>

---

## The Diverse Needs of a Diverse Industry

Online companies are spread across the economic spectrum. A network hardware company like Cisco has very little in common with AOL/Time Warner’s news and entertainment business, which in turn shares little with an Internet service provider (ISP)

---

<sup>43</sup> Robert W. Hahn, “An Assessment of the Costs of Proposed Online Privacy Legislation,” AEI-Brookings Joint Center for Regulatory Studies, Washington D.C., May 7, 2001, pp. 23-24.

<sup>44</sup> Paul H. Rubin, Senior Fellow, Progress & Freedom Foundation, Testimony before the Senate Committee on Commerce, Science and Transportation, Washington, D.C., Oct. 3, 2000, p. 5.

or Web-hosting company such as Netcom.<sup>45</sup> And yet government regulation is by necessity of the “one-size-fits-all” variety which would lump these diverse companies under the same piece of legislation.

Just as online companies reflect vastly diverse sectors of industry, so too do Internet consumers, who also have different preferences when it comes to the level of privacy they prefer. The private sector is solving this issue itself, by allowing individuals to specify whether they want to make themselves anonymous while searching online, or whether they wish to give a certain amount of their information to marketing companies as they see fit. Incorporating such nuances into a standard federal regulation would be difficult, and any resulting privacy notice would have to be exceedingly complex, causing many people to ignore them or simply refuse to go online. That argument does not mean the government should refuse to intervene if the private sector fails to provide the flexibility and technology to address privacy concerns, but it does provide a cautionary note for federal intervention.

---

## The Case for Private Sector Self-Regulation

Online commerce was the fastest growing industry of the 1990s and will continue to grow rapidly in the future. As a result, more than ever, people have access to information and resources they never would have thought possible in their parents’ generation or even a decade ago. The Internet’s simplicity and convenience have allowed people to purchase anything from household groceries to spare car parts online and have them delivered to their door. The regular use of e-mail has become the norm across generations and thousands of high tech jobs have been created, a factor which has underwritten economic growth in the 1990s.

All this activity has occurred in an atmosphere of very little regulation, allowing a fledgling industry the freedom it needed to flourish. If any legislation had been enacted at an early stage of the Internet’s development, it could have had the disastrous result of stifling the creative energy being devoted to making an Internet where all can feel safe. And this possibility is still a very real concern to an as-yet largely unregulated online community.

Large companies such as McGraw-Hill already have whole departments working solely on privacy policies to ensure they keep up to date on changes in technology. An annual report is published for customers about changes to the privacy policy and periodic audits of the policy are undertaken throughout the year to ensure compliance. There are privacy personnel employed in each business unit of the company to train people on the subject and for customer contact in case of complaints. The company has admitted that these measures have cost them millions of dollars, but have stated that they would enact them with or without regulation as it is in the customer’s, and therefore their own, best interest.<sup>46</sup> Other companies such as AT&T send an annual written privacy notice to each customer and maintain a “do not call” list of customers.

---

<sup>45</sup> <http://www.techWeb.com/news/story/TWB19980417S0024>, Accessed April 25, 2001.

<sup>46</sup> Software and Information Industry Association, Presentation to Congressional Staff, March 21, 2001.

Many other companies have said that they prefer the self-regulatory approach to the government-regulated approach, as self-regulation would give them the flexibility to respond to market forces and consumer choices, while balancing cost-benefit considerations. When it comes down to the bottom line, if the consumer doesn't like the site's privacy policy, they can vote with their mouse and leave the site.

Regulatory constraints can be a major factor in the survival of Web businesses. The Forrester Report stated that compliance costs of government legislation for the Reed Elevier/LEXIS-NEXIS group would be \$44,000 to \$1 million per year.<sup>47</sup> Privacy compliance costs real dollars, more than many businesses can afford. So why not let market forces influence industry practices instead of artificially changing the marketplace? As Americans know too well, once government intervenes in any industry, it is there to stay, and it doesn't stop at the first step on the ladder to greater control.

Intel Chairman Andrew Grove goes against the grain by supporting government regulation of what he calls "personal property" on the Internet. He believes the prospect of facing 50 state regulations and hundreds worldwide would impose huge costs on technology. While Grove has a point regarding the cacophony of laws that govern world commerce, at least in the United States the prevailing industry view regarding the Internet is that self-regulation must be given every opportunity to succeed in creating an international privacy standard before the government steps in.

The alternative to government regulation is a combination of public education, consumer pressure, new technologies, and privacy policies that act as privacy contracts. Consumer pressure can have a remarkable effect, as Amazon.com quickly learned, when it allowed customers to opt out of its "purchase circles"—a published list of purchasing patterns—after some of its customers voiced opposition. In a similar case, America Online (AOL) was flooded with protests and watched its stock sink after announcing it would sell user information. They quickly dropped that idea.

The information technology industry recognizes that protecting personally identifiable, sensitive information is important to its customers—so much so that it is often a prerequisite to shopping online. To protect such information is vital to the very survival of online businesses. Microsoft's Chief Operating Officer Bob Herbold stated that Internet privacy protection is a top barrier to the continued growth of e-commerce and that it is necessary for businesses to tackle this issue or they will see profits fall very quickly—an excellent example of market forces at work.<sup>48</sup>

The irony of the new focus on online privacy is that the Internet is one of the easiest places to control the use of personal information, particularly if attention is paid to what can be done to protect the data. There are already many tools online to protect privacy for consumers. Following are five highly effective private-sector alternatives to government regulation:

---

<sup>47</sup> Idem.

<sup>48</sup> Bob Herbold, Chief Operating Officer, Microsoft Corporation, Statement at the PC Expo, New York, New York, June 1999.

## 1. Company Policies as Effective Oversight

The number of sites which now have privacy policies has increased from 14 percent in 1998 to 88 percent last year.<sup>49</sup> Many companies provide resources for establishing privacy policies. For example, the Privacy Council offers audits, consulting services, assessments, training and seminars to help companies set up privacy policies. These seminars educate professionals, businesses and their clients and consumers on privacy issues and solutions in a marketplace that is becoming increasingly lucrative as private sector demand rises for such services. Direct Marketing Association Interactive (DMAI) simplifies the procedure further, requiring the client to fill out a questionnaire on DMAI's privacy generator. The privacy policy will then be e-mailed to the client for editing before being posted to the Web site. DMAI even allows the client to update the policy as needed. Finally, Microsoft's Privacy Wizard is a free online tool that allows businesses to create and post comprehensive privacy policies on their Web sites. It has generated 18,000 policies with 12,000 completed and 8,000 posted by Web sites.<sup>50</sup>

The scope and content of Web site privacy policies has improved as well. The Hewlett-Packard Web site, for example, has a privacy policy that is four pages and more than 2,100 words long.<sup>51</sup> Amazon.com has a 1,500-word policy that includes the ability to set Customer Communications Preferences.<sup>52</sup> Both Web sites explain what they do with the information that consumers provide; how they collect and use it; whether or not the information is shared with others and how consumers can control that process; how they use cookies; the security of transactions; and other policies that affect online activities.

Many Internet companies have gone to great lengths to protect the privacy of their visitors and thereby exposed themselves to liability if they fail to live up to their promises. They know privacy is good business. Moreover, some large companies, including IBM and Walt Disney, take the issue so seriously that they do not advertise on sites that do not post privacy policies.

## 2. Seals

The second tool the online industry is using to regulate itself is the seal program. A seal is validation by an independent, trusted third party which can be used to connote both compliance with privacy policies and an easy method for consumers to contact the seal provider. This technology is ideal for small businesses, which often don't have the resources to fund entire privacy departments.

A seal will establish that a Web site's privacy policy is accurate, comprehensive, prominently displayed, completely implemented and accessible. It also alerts consumers to the complaint resolution mechanisms through which complaints are handled. Periodic reviews or auditing of certain sites are also used to maintain compliance. Notice can be

---

<sup>49</sup> Software and Information Industry Association, Presentation to Congressional Staff, March 21, 2001.

<sup>50</sup> Richard Purcell, Director, Corporate Privacy, Microsoft Corporation, "Delivering Customer Trust at Microsoft," March 2001.

<sup>51</sup> <http://www.hp.com>.

<sup>52</sup> <http://www.amazon.com>.

given to the site if it is no longer compliant with the standards, and this information can be made a matter of public record.

The Online Privacy Alliance (OPA) supports this type of protection, stating that seal programs should be objective and build legitimacy with consumers. Seal providers should solicit and consider input from the business community, consumer/advocacy organizations and academics in formulating their policy. The OPA suggests that seal providers should make their seals accessible, affordable (especially to small businesses), and comprehensive enough to cover sensitive and non-sensitive information. The OPA also suggests that seal providers be able to handle consumer inquiries and complaints and that its seal be widely used and recognized.<sup>53</sup>

TRUSTe<sup>54</sup> and BBBOnline<sup>55</sup> are examples of accepted seal programs, which certify that member Web sites have a privacy policy that adheres to certain minimum standards. BBBOnline is literally the Better Business Bureau online, and TRUSTe is a nonprofit rating organization created by CommerceNet, the Electronic Freedom Foundation, and a few dozen e-commerce corporations. TRUSTe conducts tests on member sites to ensure continued compliance with its standards, and allows its logo to be displayed on the member's homepage. It also tests on a regular basis to make sure the site is following up on its own policy. Member companies are bound by a legally enforceable contract to follow their own privacy statements.

### 3. Education

Consumer knowledge of privacy online is sorely lacking. In order to prevent the government from stepping in to "protect" consumers due to their own supposed ignorance, the private sector must do a better job of educating online visitors. Despite the already existing system for protecting private information, concerns about Internet transactions have grown. People will lock up their cars before leaving them on the street, but there is little understanding as to what they need to be secure on the Internet.

There is a Big Brother fear that some unknown entity is gathering information and nothing can be done about it. This fear is mostly linked to the dissemination of secondary and aggregate information, rather than the primary information the citizen knowingly gives to parties such as a doctor or accountant. The unease may be rooted in e-commerce's impersonal nature (one can argue directly with customer service in a store or with a credit card company on the phone if a transaction goes sour), and the stark reminder that one is entering a "secure" area when making purchases. Legislators may exploit these fears of an Internet "eye in the sky" to push through draconian legislative measures.

According to Forrester Research, 65 percent of consumers are "very concerned" or "extremely concerned" with online privacy, and those fears led to a loss of \$4.2 billion by e-commerce companies in 1999.<sup>56</sup> The Pew Internet & American Life Project also

---

<sup>53</sup> <http://www.privacyalliance.org/resources/>, Accessed April 25, 2001.

<sup>54</sup> <http://www.truste.com>.

<sup>55</sup> <http://www.bbbonline.com>.

<sup>56</sup> <http://www.zdnet.com/eweek/stories/general/0,110011,2662502,00.html>, Accessed March 21, 2001, p. 2.

released a study in July 2000, which stated that more than half of Americans would want new laws to protect themselves from government and other kinds of unwanted surveillance online, and less than a third trust government officials to make the right choices.<sup>57</sup>

Several Web sites, such as NetPrivacyPower.org, are already educating the public about online privacy through consumer campaigns by providing information about how to protect yourself online, including how to verify your browser security level, browse anonymously and reject unwanted cookies.<sup>58</sup> Dell has an “E-ssentials” campaign with advice on keeping your password secret, understanding financial security on the Web, avoiding viruses, and viewing your rights on the Web.<sup>59</sup>

Companies like Privada teach seminars on how to write privacy policies.<sup>60</sup> These training entities have observed that in the last few years, companies have changed their attitudes towards such policies and incorporated them into their Web sites, while also changing what they define as sensitive information and protecting it to a greater degree.

Microsoft is promoting an educational campaign to inform consumers with privacy statements that are simple to find and written in clear and understandable language. As a result, customers will be able to easily review and change their information.

## 4. Browsers and Cookies

The fourth security tool available in the online industry is browsers and cookies. All browsers can be set to accept all “cookies,” be prompted to accept some cookies, or be set to disable all cookies. For those not familiar with the Internet, these cookies are inedible—they are actually pieces of text that enable Web sites to identify repeat visitors. When a consumer returns to the same Web site, their own computer sends back the cookie, letting the site know they are back. Cookies have a unique identifying number, which lets the Web site keep track of what they do on the site. It may lead the consumer to the area they visit most frequently, or even provide an ad that addresses their personal interests.

Secure Socket Layer (SSL) browsers display a security icon—a locked padlock in the lower left corner of the window for example—to indicate a secure site. These browsers also determine whether the receiver of an e-mail is an imposter by asking for a certificate issued to the site by a Certification Authority (CA) such as Equifax, GlobalSign or VeriSign.

While cookies sounds quite Orwellian, the information they contain is initially limited to the user’s online provider’s server and his or her type of browser and computer. Accepting a cookie does not give a Web site access to any personal information, other than the data one chooses to share with the company. Additional information comes

---

<sup>57</sup> <http://www.zdnet.com/eweek/stories/general/0,110011,2662502,00.html>, Accessed March 21, 2001, p. 2.

<sup>58</sup> <http://www.netprivacypower.org>, Accessed April 26, 2001.

<sup>59</sup> [http://www.dell.com/us/en/gen/misc/policy\\_000\\_policy.htm](http://www.dell.com/us/en/gen/misc/policy_000_policy.htm), Accessed April 26, 2001.

<sup>60</sup> <http://www.privada.com/enterprises/index.html>, Accessed April 26, 2001.

from the user, through registration at a Web site or purchase of a product that includes personal information.

If one wishes to keep such information private, there is usually a way to control how much personal information is shared, such as not providing any of it at all, or checking a box indicating one's preference. Some companies state clearly they will not share the information, but will use it only to provide additional product information or special offers. This increases the efficiency and effectiveness of a visit to a Web site, and often leads to specific responses geared to one's specific interests (somewhat like an online salesperson).

If this process makes people uncomfortable, it's not a good reason to avoid going online. It is a good reason to take the time to change browser preferences to disable cookies or be alerted when cookies are being sent. It is possible to simply edit and/or delete cookies from computers without causing any harm to your system. Cookie managers and blockers exist in every browser on the market. Companies will even educate users as to how this can be done via their privacy policy—where one can learn how to control which cookies to accept, how to access cookie files and how access to that site would be affected if cookies were refused.

Fear about cookies is unfounded. Amazon.com, for example, uses them to personalize the log-in page, make suggestions regarding the type of books one might like to read, respond to requests, customize future shopping, improve their online store, study market trends and improve productivity.<sup>61</sup> This targeted marketing provides customer content and relevant information to the buyer. Just imagine if the real world were organized that way and one was able to walk into Macy's or any other store and immediately find similar purchases to those made in the past, in a range of colors and all in the right size at the front of the store. Cookie personalization makes this possible online.

However, no amount of personalization will make people shop online if their security is compromised. Amazon.com, for example, shares personalized information only with third party companies that deliver services such as fulfilling orders, delivering packages, analyzing data and providing marketing assistance. Beyond those obvious needs, Amazon.com will give the consumer notice when the information may be shared with other third parties, and the consumer has the option not to share that data. Hewlett-Packard states in its privacy policy that it will not "sell, rent, or lease your personal identifiable information to others" and that "your permission is always secured first, should we ever share your information with third parties that are not acting on our behalf and governed by our privacy policy."<sup>62</sup>

It is in this way that the private sector has responded to consumer demand for secure online transactions and protection of personal information. These and other Web sites and others legitimate the tracking of consumer information, limit the collection of information to strict marketing purposes for consumer convenience and do not share the information to third parties without express consumer consent. In this manner, private

---

<sup>61</sup> <http://www.amazon.com/exec/obidos/tg/browse/-/468496/105-0332609-2899965>.

<sup>62</sup> <http://www.hp.com/country/us/eng/privacy.htm>, Accessed April 25, 2001.

companies track consumer information to better serve customers; governments may have other purposes.

## 5. Private Sector Protocol (P3P) and Other New Technology

Fifth in the list of private sector alternatives, the development of new technologically advanced tools gives individuals greater control over their personal information. A widely supported effort is P3P, which stands for Platform for Privacy Preferences. It was engineered at the World Wide Web Consortium (W3C), a consortium of 434 members, including the largest players in the Internet, such as AOL, Cisco and Microsoft. P3P enables Web sites to express their privacy practices in a standard format that can be retrieved automatically by user software "agents." This represents a broader approach than simply controlling cookies.

P3P communicates the user's privacy preferences to the Web site the user is currently viewing, laying down the limits to which the user is prepared to divulge personal information. A user could provide the Web site with past purchasing information, for example, but refuse to give an address or telephone number. This gives the user complete control and choice over how much and what kind of information is given to each Web site.

There are many other innovative methods to protect privacy. Network Associate's Net Tools Secure Suite provides encryption, authentication, policy management, anti-virus, and intrusion-detection technology, mostly for commercial users. Anonymizer allows one to surf anonymously, by providing an untraceable alias, offering anonymous e-mail and Internet access.<sup>63</sup> Freedom is a similar company that will charge \$50 a year to provide up to five online aliases and allow anonymous profiles. Freedom is a product of Zero Knowledge, a Canadian company based in Montreal, and does not have to follow U.S. law. As a result, it can use stronger encryption than similar American products.<sup>64</sup> Bell labs and AT&T have developed "Crowds" which uses a virtual "crowd" of people to hide one's identity while surfing. Users are placed in random groups. Each time one instructs a browser, the command is randomly routed through the machine of someone else in the group so that it is impossible to track a group member individually.<sup>65</sup> The Onion routing system, under development by the Naval Research Laboratory, keeps third parties from tracking surfing activities by randomly moving messages through a series of routers before the message reaches its destination.

One of the most inventive of the emerging technologies is Lumeria, a site that hides individually identifiable data and then allows the user to charge companies to see it.<sup>66</sup> This California-based company believes that if personal information is valuable to businesses then they should pay for it. The free portion of the new service can also place users on a "do not contact" list for direct marketers.

---

<sup>63</sup> <http://www.anonymizer.com>, Accessed April 25, 2001.

<sup>64</sup> <http://www.zeroknowledge.com/privacy/default.asp>, Accessed April 25, 2001.

<sup>65</sup> [www.research.att.com/projects/crowds](http://www.research.att.com/projects/crowds), Accessed April 25, 2001.

<sup>66</sup> [www.lumeria.com](http://www.lumeria.com), Accessed April 25, 2001.

Hailstorm is a service being developed by Microsoft which is oriented around users, instead of a specific device, application, service or network, taking advantage of the .NET technologies and architecture that make it possible for applications, devices, and services to work together.<sup>67</sup> It creates an information “hailcloud” in which all personal data is stored—an electronic address book, contacts, calendar, documents, wallet, favorite Web sites—all of which are interconnected and can be accessed from anywhere at any time. Adding a friend’s phone number on one’s cell phone will also update that information in one’s computer, for example. Making an airline reservation online will automatically register the travel details onto the online schedule, inform the travel agent of the relevant frequent flyer number, window or aisle seating preference and whether a special meal is required.

Another product allowing individual control of information is “DigitalMe,” which stores the user’s personal data and uses it to fill out forms at Web sites automatically, allowing a final review before they are submitted. The software, available by download in June 2001, will keep track of passwords and names used from site to site.<sup>68</sup>

Hailstorm, DigitalMe, Onion, Crowds and other new technologies turn the argument over online privacy on its head. Instead of debating how much organizations can get away with in respect to an individual’s information, they start with the assumption that the user controls all personal information and decides with whom to share it and under what terms. Any access, changes or use of that data require the explicit consent of the user as the ultimate decision-maker. These new technologies provide an arsenal of arguments against any politician intent on Internet privacy regulation.

---

## Conclusion

The federal government and the private sector face many challenges with regard to information privacy. Federal government agencies are increasingly exchanging and merging personal information. On average, a new program for comparing databases is announced every two weeks.<sup>69</sup> But continued failure to comply with existing government privacy standards will lead to more bureaucracy and easier access to information that will tempt many to violate shared personal information. Federal invasion and abuse of personal privacy via computer databases is no less a crime than breaking into one’s house without a warrant or taking property without due process, which are specifically outlawed by the Fourth Amendment. The framers of the Constitution recognized the unique powers of government and sought to curtail them by preventing governments from collecting information about citizens without substantial justification. At the very least, the federal government should adopt the new security technologies prevalent in the private sector to reduce the exposure of personal records to unwanted eyes.

Given the pitfalls of having the government make decisions about control over personal information, it would behoove the public to spend time exploring the many technologies

---

<sup>67</sup> <http://www.microsoft.com/net/hailstorm.asp>, Accessed April 20, 2001, p. 3.

<sup>68</sup> [www.digitalme.com](http://www.digitalme.com), Accessed April 25, 2001.

<sup>69</sup> “Privacy and Federal Agencies: Government Exchange and Merger,” <http://www.privacilla.org>, March 2001, p.

already available to protect personal data and behoove the technology industry to prominently cite its self-regulating activities. Much of the e-business community, including Hewlett-Packard, Intel and eBay, supports the requirement of a prominent notice of a Web site's privacy policy and a check box to opt out of information collection. President Bush has embraced such "notice and consent" policies. In fact, of the top 100 private sector Web sites, 97 to 98 percent are compliant with their privacy policies without any legislation.<sup>70</sup>

To date, the private sector has shown greater concern than the federal government over being a guardian of people's privacy. For the government to regulate the private sector while its own house is in disrepair and without sufficient evidence that such action is absolutely necessary would be costly to the economy and an enormous waste of taxpayer money.

As with any other issue, the more that individuals do to control their own lives—in this case personal information—the less need there will be for Big Brother to put a cop on every cybercorner. The private sector will continue to respond to consumer demand for improved privacy protection, and will move even faster if it believes the government will legislate or improve regulatory constraints on how e-commerce is conducted. As the Internet's influence on society grows exponentially, ensuring one's privacy will determine whether or not the Internet becomes a vital medium for commerce, business and entertainment or whether the government will step in and stifle freedom and innovation. In the end, whether the issue is privacy, Internet taxes, or antitrust policy, the further offline the government stays, the better off all Americans will be.

---

<sup>70</sup> Software and Information Industry Association, Report and Presentation to Congressional Staff, March 21, 2001.