

THE INTERNET PRIVACY DEBATE

by

Kenneth Brown *

"The whole of science is nothing more than a refinement of everyday thinking."

- Albert Einstein

A. Introduction

A study conducted by the Angus Reid Group, "The Face of the Web," found that more than 300 million people are already on the Internet, and as many as 150 million more are planning to go online during the year 2000. In a relatively short amount of time, the Internet has become a ubiquitous tool throughout the world.

However, for all of its convenience, the issue of privacy has become a nemesis for advocates of the new technology. Activists, regulators, courts, local and international governments insist that the current Internet model too freely violates individual privacy rights. Deborah Pierce, counsel for the Electronic Frontier Foundation, estimates that there are over 3000 bills in both local and federal legislatures around the country concerning Internet privacy. Many predict privacy concerns and the Internet are on an inevitable collision course with strict governance and legislation.

Privacy advocates insist on a wide range of remedies. Recommendations range from web-safety notices to strict "policing" to monitor the exchange of personal information on the net. Although all parties agree on the need for privacy on the net, the difficulty rests in how to effectively regulate the net to achieve privacy. Unfortunately, differences among experts about how to regulate the net are as contentious as the concern about privacy.

Privacy itself is particularly complicated in the U.S. because historically it is not referenced nor mentioned in the U.S. Constitution, the Bill of Rights, nor its Amendments. Privacy and the "right to privacy" are loosely defined. The Internet is a new technology with infinite capabilities for information exchange. Privacy and the Internet combined easily become a hydra of issues, including disagreement over regulatory effectiveness, anonymity and uncertainty over the adverse impact of regulations on the Internet economy. Closely reviewing the issues reveals the complexity of the privacy debate.

* President, Alexis de Tocqueville Institution.

B. DoubleClick- The Beginning of the Controversy?

Internet privacy has always been a topic of heated discussion. However, many would agree that the DoubleClick debacle earlier this year brought world attention to the Internet privacy debate. DoubleClick, founded in 1996, spawned from the growing demand for effective accountable advertising on the web monitoring by Internet advertisers. DoubleClick combines technology and media expertise to enable clients to better target Internet audiences. With DoubleClick's ad delivery, dotcoms receive reports about average age and income of surfers, which visit their site as well as information regarding the frequency of daily and monthly visits by customers. DoubleClick's clients include Toyota Motors, Popular Mechanics magazine and even The Washington Post.

As DoubleClick's customer base grew, the company decided that it would improve the value of its service to customers by combining its ad delivery technology with a customer database list from a company called Abacus Direct. Reporter Jeffrey Rosen, in a New York Times magazine piece (April 30, 2000), summarized the controversy, "As long as users were confident that their virtual identities weren't being linked to their actual identities, many were happy to accept DoubleClick's cookies (small packets of specific personal data stored on consumers' computers) in exchange for the convenience of navigating the Web more efficiently. Then last November, DoubleClick bought Abacus Direct, a database of names, addresses and information about off-line buying habits of 90 million households, compiled from the largest direct mail catalogs and retailers in the nation. In January, DoubleClick began compiling profiles linking individuals' actual names and addresses to Abacus's detailed records of their online and off-line purchases. Suddenly, shopping that once seemed anonymous was being archived in personally identifiable dossiers."

DoubleClick's effort to enhance its capabilities was met with furious outcry. The ACLU, the Center for Democracy and Technology, and scores of consumer advocates launched an almost fatal attack on DoubleClick. Wall Street responded to the controversy by sending the company's stock from a high of \$135 to a low of \$83.

After months of controversy, on March 2, DoubleClick ended its pursuit to combine the Abacus database with its technology. In a public statement to end the controversy, Kevin O'Connor, CEO of DoubleClick remarked, "The overwhelming point of contention has been under what circumstances names can be associated with anonymous user activity across Web sites...It is now time for industry, consumers and government to develop a clear set of guidelines that help create a healthy, free Internet while protecting the privacy of all consumers." Despite O'Connor's appeal, the controversy ignited an irreversible furor over Internet privacy.

C. Regulatory Debate Over Privacy

In response to the demand for government involvement, on March 15, 2000 Rep. Asa Hutchinson (R) and Rep. Jim Moran (D) introduced a bill for a federal privacy commission that would decide how new privacy regulations should apply to corporations, which collect customer information on the net. Fordham University Law Professor Joel R. Reidenberg, advocating the

measure, told a House Subcommittee May 18, "...To protect Americans' privacy, the government must establish a full-time body that can offer constant vigilance, expertise, and judgment."

Dissenting, Rep. Bob Goodlatte (R-Va.) accused Reidenberg of "...advocating the establishment of unnecessary, massive federal bureaucracy and the imposition of a complex set of regulations not only on sophisticated commercial entities, but also on anyone who had the means and inclination to put up a web site." Ken Johnson, spokesman for Rep. Thomas Bliley (R-Va.) echoed members' concern about wide-sweeping privacy measures, commenting, "the quickest way to kill the Internet is to regulate it to death."

N.Y. Attorney General Eliot Spitzer, who in January succeeded in halting Chase Manhattan Bank's practice of selling its customers' personal information to third-party marketers, highlighted his skepticism, commenting, "I don't believe that the government should, or is wise enough, to say what information should be considered public and what should be considered private...I do believe that decision should be left up to consumers..."

Current legislation in Congress focus upon different aspects of Internet privacy. Senators John McCain (R-Ariz) and Senator John F. Kerry (D-Mass.), Senator Ernest F. Hollings (D-S.C.) and Senators Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.) have all introduced Internet privacy bills. However, opponents of each bill disagree over innumerable items including Federal Trade Commission enforcement powers, privacy policy notification measures, and even "opt-in, opt-out" measures for consumers. While consensus is that an Internet privacy bill will be passed, the intense opposition to data collection on the Internet coupled with the concerns over the policing of the net signal perpetual debate over Internet privacy in Congress.

D. The Privacy Controversy and the FBI

Meanwhile, disagreement on privacy measures has also brewed between the Department of Justice and the U.S. Congress. Discussing security on the Internet, U.S. Attorney General Janet Reno hinted that the FBI and other government agencies needed to have a way to penetrate anonymity and trace criminals who hide their identities online, which also fueled widespread alarm among privacy advocacy groups. House Majority Leader Dick Armey commented, "The Administration is full of double-talk on Internet privacy...While the President lectures the IT industry about the importance of privacy to consumers, his Administration wants to let "Big Brother" track our every move on the Web." Immediately, privacy advocates put the FBI and other law enforcement agencies under siege.

Virus outbreaks, fraud, and security issues have put law enforcement officials in the awkward position of utilizing Internet monitoring techniques to detect and track crimes in cyberspace. Regardless of its good intentions, the FBI's disclosure of its use of surveillance software (dubbed "Carnivore" because of its enhanced ability for compiling Internet data) prompted Congress to hold hearings specifically on the use of "Carnivore" as a law enforcement tool.

In surprise turn of events, on August 2, U.S. District Judge James Robertson upheld Electronic Privacy Information Center's complaint that the FBI was obligated to submit a plan to expedite its fulfillment of EPIC's Freedom of Information Act (FOIA) request for details of

"Carnivore's" information gathering abilities. EPIC spokesperson David Sobol commented, "The deployment of Carnivore is the latest indication that legal protections have failed to keep pace with advancing surveillance technology. The existing wiretap statutes, which were drafted with telephones in mind and amended in 1986 to apply to electronic communications, do not adequately address many of the realities of the Internet." The FBI commented that, "...they hope to assuage the fears of civil libertarians" through "an independent verification and validation" of Carnivore's eavesdropping system.

E. Conflicting Views of Anonymity in Courts

Coupled with disagreement among government officials, the Internet privacy debate has also become the subject of hundreds of court cases around the country. The American Civil Liberties Union (ACLU), EPIC and other groups have sued web portals for releasing identities of users in response to subpoenas. Even with proper notification, activists are against the release of Internet users' identities, citing Supreme Court rulings, which support anonymity in free speech such as *Talley v. California* in 1960 and *McIntyre v. Ohio Election Commission* in 1995.

However, many judges (and juries) are in disagreement with freedom of speech arguments. In May, Dade County, FL Circuit Court Judge Eleanor Schockett ordered AOL and Yahoo! to divulge the identity of an anonymous message writer sued for defamation by Fort Lauderdale businessman J. Erik Hvide -- ruling, "... J. Erik Hvide has every right to face his accuser...the Internet cannot be a shield for libel or slander."

Legal questions of libel and slander have led to a surge of lawsuits in courts. Corporate Counsellor Newsletter reported, "...the Silicon Investor, an investment website featuring advice and chatrooms, receives about one subpoena a day seeking the identities of authors of message board postings." Professor Lyrrisa C. Barnett Lidsky, Associate Professor of Law at the University of Florida commented, "There has been a tremendous explosion of cases in the last six months. If courts lower the bar in granting subpoenas, it will nullify the existence of any privacy on the net. Each time a new subpoena is issued, the defendant's right to privacy is violated."

New legal interpretations of the law call into question the effectiveness of the courts to uphold "the right to privacy." Deborah Pierce, counsel for the Electronic Frontier Foundation (EFF), commented, "I think that the court and Congress have been moving in opposite directions on privacy for the past 20 years... Congress has definitely latched onto the privacy issue. And the courts have been mechanistic in applying the law but their decisions are not really applicable to the current state of affairs on the net."

The pace of change in the technology industry presents the utmost problem to legal edict. Stuart M. Benjamin, Associate Professor at the University of San Diego Law School, argues, "Some people might say: 'well, we don't care if the facts have changed....we want the Supreme Court and Courts of Appeals to make pronouncements of law,' but important legal decisions based on stale facts do a disservice to both parties in a dispute. The Internet's challenge to the appellate process is profound..."

F. Investor and User Confidence and the Privacy Debate

While the privacy debate rages across the country, the concerns have impacted consumer use of the Internet. A recent study confirmed that the perception of lost privacy on the Internet dramatically slows e-Commerce. Jupiter Communications, a leading Internet and e-Commerce research company, noted in June of 1999 in a report entitled " Proactive Online Privacy: Scripting an Informed Dialogue to Allay Consumers' Fears" that analysts predicted a \$18 billion revenue drop in consumer e-Commerce transactions due to privacy concerns. Economics Professor Andrew Sellgren of George Mason University commented, "Consumers will become more and more discouraged from purchasing goods and services over the Internet if complex and burdensome regulations complicate their transactions or if there is a continual news-drumbeat that the Internet is unsafe to use...If we are not careful the very product we created will become nothing more than a useless tool."

Along with Washington and the courts, the difficulty of reaching agreement on regulatory measures is attentively being watched by Wall Street. Because of its narrow margins and highly leveraged operations, investors are particularly watching the Internet regulation. James Lucier, senior analyst with Prudential, commented, "Legislation is the newest metric Internet investors have to deal with. Not only is the number of laws at both the federal and state level that directly affect the Internet and online business growing at the same rate as other Internet metrics, but it is also the one to most worry about. As a general rule, any Internet-specific legislation beyond the minimum necessary to ensure the enforcement of contracts imposes costs and retards innovation. Similarly, regulatory costs do cut into corporate profits, but what worries us most is the threat to "biodiversity" on the net that is posed by regulatory barriers to entry. About 50 percent of US GDP originates in small companies employing 100 people or less. These are for the most part companies that can barely cope with the costs of high speed internet access, let alone the costs of multi-state tax compliance should the fact of being active on the net subject them to the tax and regulatory regimes of every political jurisdiction in which their customers do business."

The Microsoft legal battle illustrates the relationship between investor confidence and Washington. The news of the collapse of settlement talks in the Microsoft case caused the software giant's stock to plunge nearly 15% and pushed the NASDAQ Composite Index almost 8% lower. A study published by George Bittlingmayer and Thomas W. Hazlett of the University of California reported the link between investor confidence in Microsoft and government regulation. The study analyzed investor reactions to 37 antitrust actions affecting Microsoft from 1991-1997 and their effect on the index of 159 other computer-related companies. Their findings confirmed a strong negative correlation between regulation and the stock market: news of Microsoft's setbacks depressed technology stocks, while news of Microsoft's victories in antitrust suits increased the price of technology stocks. In an interview for Business Week, Bittlingmayer remarked, "Although some investors may think Microsoft engaged in anticompetitive behavior, most believe that the whole technology boom has been fostered by the absence of government regulation. And apparently they have little faith that the government can intervene in an efficient way--especially when the computer market is changing so rapidly."

G. Marketing and the Privacy Debate

A helpful perspective of the privacy debate is looking at its pre-Internet history. The "identity-data" industry is over one hundred years old. One of the first companies to collect and sell this information, Equifax, headquartered in Atlanta, GA, began compiling and selling personal consumer information files in 1899. Today, millions of marketers, businesses, and intermediaries buy personal databases from companies similar to Equifax.

For example, ACXIAM, based in Little Rock, AR, sells personal database files for as little as \$.10 a name. For just \$20, ACXIAM customers can buy one thousand names for any geography specific to a five-mile radius of any street address in the U.S. For varying prices, ACXIAM will sell lists of names specific to hundreds of descriptions such as ethnicity, banking information, number of household children, yearly income, recent purchasing habits or even marital status.

The benefit of target market data and customer lists will remain an incentive for firms to collect it. Alternatively, companies would have slow, expensive methods of reaching customers, costs that would inevitably be passed to the consumer. Customer data provides marketers with an effective way of targeting their stay out of the damaging hi-beam accusation of being a privacy violator, but it collects valuable information about potential customers. The appearance of unlawful or inappropriate data collection is a financial and public relations nightmare as seen in the DoubleClick incident. Dave Mooney, legal counsel for Equifax comments, "Equifax has built our good reputation through a commitment to protecting the privacy...we continue to survey consumers on their privacy concerns so that we can address them."

H. Self-Regulation, Partnership and Improvement of the Internet

Because an information society depends upon perpetual data collection, personal privacy, anonymity and protection will always be of concern. An information society's members (and users) will inevitably make the necessary adjustments to work together. Industry leaders at hundreds of companies including Amazon.com, eBay and America Online are independently urging hundreds of e-commerce companies to take the initiative in ensuring that Internet firms establish and promote the adoption and implementation of rigorous voluntary privacy policies. They are also asking e-commerce ventures to urge

Internet surfers themselves to scrutinize the privacy policies of the Web sites they visit or conduct business through.

The economics of fraud, consumer complaints and profits have prompted American Express, MasterCard, and Visa to independently take action to stem credit card abuse on the Internet. MasterCard and Visa have come up with a rating system that rewards responsible e-Commerce businesses with preferential treatment and penalizes those that engage in high-risk behavior. Frank Williams, vice president of fraud at Visa commented, "We have an international program in the pipeline which will mean all acquirers (merchants' banks) of Visa cards will have

to ensure that merchants' web sites are secure." This is in addition to new ratings systems, heavily penalizing merchants that engage in high-risk e-commerce. "

As reported in Interactive Week, Internet entrepreneur Mark Hudson was ready to launch an online dating site in late March, but abruptly changed his mind when he found out that his business idea was considered "high risk" (defined as an unacceptably high rate of disputed credit card charges) and could open him up to potentially huge fines by Visa and MasterCard. Likewise, American Express announced in May that it was exiting the digital adult content industry because of declining profits – due to the high dispute rate surrounding adult online activities, American Express was facing high administrative costs and decided to withdraw its credit from the industry.

Former Commerce Secretary William M. Daley commented, "Privacy is not as important as other issues. We've spent a great deal of time working on privacy and consumer protection concerns, but to be frank with each other, what is an even more basic concern to consumers is the issue of security..." The Clinton administration recently stated: "Internet businesses, many of which have long been suspicious of government regulation, need to cooperate with law enforcement to fight online crime. Rather than foster powerlessness by denying consumers the ability to choose, a stronger government-industry partnership aimed at Internet security would be the best compromise." Today, almost all experts are recommending improved security technology, enforcement of existing laws, and enhanced cooperation between the authorities and the computer industries.

The G8 countries and seven others including Scandinavian states and Brazil have already set up a network of police contact offices open around-the-clock to exchange information and field requests for action against cross-border cyber criminals. With the spread of the "ILOVEYOU" virus and several others only days later, businesses and governments are quickly realizing that they must team up in order to catch and punish Internet community vandals. Detering cyber crime will face many difficulties. But businesses are expressing an avid interest in this ongoing process. "CEO's must personally involve themselves in security and privacy," said Jeff Richards, executive director of the Internet Alliance, an industry group based in Washington. "I think legislation in this case should be generally a last resort.... An industry-wide commitment to boosting cyber-security would also enhance consumer confidence. "

Recently, an international public-private dialogue led to a meeting of about 300 government and industry representatives aimed at stemming computer viruses (such as the much-publicized "ILOVEYOU" virus), hackers who steal or distort information, and criminals who defraud online shoppers. The convention, which the French government proposes should become a worldwide pact against cyber crime, would require all signatory countries to harmonize their laws and decree tough punishment - including extradition - for cross-border hackers.

William Hague, leader of the Conservative Party in the UK, in an interview with Sili-con.com, concurred. "We've got to make sure there's a balance in regulation but I think we should err on the side of freedom. I think one of the great things about the growth of the Internet is the freedom that it is giving people - the freedom for people to be able to work in a new

way, the freedom to communicate with anyone in the world. And so we must cherish that freedom and not allow it to be trampled on by excessive government regulation."

I. Market Solutions to Privacy Concerns

Companies engaged in e-commerce are marketing products to increase user confidence as well provide consumer protection. In July, Microsoft announced new cookie management features for Internet Explorer, which would alert consumers when cookies arrive, as well as offer easier ways to manage and delete cookies. Bill Lockyer, California Attorney General commented, "Protecting consumer privacy is a priority; these changes to Internet Explorer 5.5 will be an important step in reaching that goal."

In many ways, the net is yielding its own self-correction for privacy concerns.

While companies such as anonymizer.com, hushmail.com and ziplip.com offer various services to allow people to surf the Net or send e-mail without being traced, software such as "Freedom" allows users to surf freely without being linked to real world identities, by encrypting their web browsing, e-mail and chatroom participation.

New innovative websites have anonymous capabilities or user identification policies. Other technologies suggest the evolution of a "caller-id" model for the Internet – where users can scramble their identities or bar communications with users who do not identify themselves. Hundreds of companies are creating software, hardware and filtering services for consumers interested in privacy. Commenting on their new Internet privacy service designed to filter content and block ads and cookies on the Web, Sam Curry, security architect at McAfee.com, summarized Internet safety reminding users, "This product is really part of a larger security solution. We recommend having anti-virus solutions to protect against bad code, a firewall to protect against hackers, and a privacy service to deal with bad content." Dov Smith, spokesman for Zero-Knowledge who are the developers of Freedom software, commented, "Our software increases user confidence, we hope to see increased use as consumers become aware of measures to protect their privacy."

J. The Future

Regulating technology has never been easy and regulatory headaches have plagued almost all industries with dynamic technological change. From pollution control standards to health and safety restrictions, regulators at the EPA, OSHA, FDA, and FCC constantly battle to keep regulatory standards up to date with recent technological developments.

The recent vote by the U.S. House of Representatives to extend the current moratorium on Internet taxes for an additional five years was a victory for U.S. technology companies and innovation. Rep. Lloyd Doggett (D) commented, "Electronic commerce is still very much in its infancy, and if we burden it with regulations, if we over-burden it with taxes, it will not be able to expand and achieve its full potential."

Einstein understood that science, innovation and technology demand a "refinement of everyday thinking." The Internet is not risk-free, particularly because of the furious pace of its advances. But like all new technologies, the light bulb, the automobile and even fire, once new technologies are studied and understood, they become reasonably safe to use. All new technology must go through its cycle of public debate over consumer safeguards. In time, the debate on the Internet will move from privacy to concerns about new technologies--and in the spirit of Einstein, we will be forced to rethink its purpose and its use. Meanwhile the privacy debate should be discussion, not panic. Regulators, courts, the private sector, and even consumers must focus on the Internet era's rewards to create reasonable, cost-benefit mechanisms to handle privacy concerns.

K. Some Important Considerations on Privacy

- 1) Unfortunately, although privacy is important, because of the inability to narrowly define privacy or the "right to privacy," there will not be a single-policy "cure-all." Willing consumers that wish to participate in marketing campaigns will continually spar with consumers that want restricted use of information they provide. Congress will seek regulatory measures to increase privacy, while the FBI, courts and other facets of government will argue against 100% anonymity. While compromise between regulators and the private sector is expected, it will not expunge concerns. Comprehensive education about the Internet and privacy tools will outrun regulatory efforts in achieving harmony.
- 2) The Internet is still new and very fragile. Too large a percentage of the Internet is either highly leveraged or unprofitable. As seen in the Visa, MasterCard and Amex cases, intense demand for profits is already increasing safety requirements for e-commerce on the web. However, consumer confidence is critical for growth. A decrease in investment will subsequently decrease investment in encryption software, etc. for Internet user security.
- 3) The information age will inherently couple privacy concerns; but that is a positive. As long as there is demand for Internet services, privacy measures will evolve to accommodate user demand.