Privacy and the Internet: the case of DoubleClick, Inc.

Scott Chapman and Gurpreet Dhillon
University of Nevada, Las Vegas

> "With growing frequency, information about how you use the Web – the sites you visit, search terms and other queries you make, online purchases, 'click through' responses to advertisements – is being captured by advertising networks or 'profiling companies.' With the permission of the Web site, but not your permission, these companies place a tag on your computer. This tag – or identifier – is then used to track your movements as you surf the Web. In addition to long lists of collected information, a profile may contain 'inferential' or 'psychographic' data – information that the company infers about you based on your surfing habits. From this amassed data, elaborate inferences may be drawn, including your interests, habits, associations and other traits."
>
> -- The Center for Democracy and Technology (CDT, 2000)

INTRODUCTION

With the advent of the Internet, a number of issues have surfaced that are affecting our society positively, negatively and confusingly at break-neck speeds. The issues surrounding an individual's right to privacy on the Internet is one such issue. Affording an individual a right to privacy is most definitely a unique right preserving the quality of the Constitution of the United States. Certainly the Internet has blurred an already gray line that Courts have fought hard and long to preserve and define over the past two hundred twenty-five years.

Once it was thought that one could not legally invade another person's privacy without a specific consenting act on the part of the invaded party barring court order. However, since the Internet has come into common use, the question now comes before us, "Is access to the Internet an act of giving up ones right to privacy?" or "Are we still afforded the same rights to privacy as traditionally held?" Surely, this question is not answered simply and, in fact, approaches so many different levels that the question itself does not even accurately frame the issue. Instead, the stage is still forming and the actors are just coming forward. The discussion in this chapter merely attempts to better define some of the blurry issues, bringing us closer to an understanding, of how this new technology should fit into our traditional beliefs in a right to privacy.

The Internet has become a new locus for social interaction and communication on a global basis. The Internet, by its nature is decentralized, open and interactive. It allows

users to publish information, engage in commerce, communicate, research and even interact on levels only previously imagined in private and intimate settings. There are no barriers to geography, society and political community. As the Internet continues to grow and allows for fully integrated voice, data and video transfer at optimal rates of speed, it will quite literally become a virtual face-to-face social, commercial and political environment.

As for today, the Internet exists within social, technological and political arenas. The technology is progressing to a point where entities can gain access to information at their every whim. Implementation of such technological advances raises significant concern by all involved. Assuredly, everyone that interacts with the Internet has concerns of privacy. Whether it is a government that worries about national security, a bank that worries about financial record accuracy, a business that worries about balancing economic potential with anti-competition impulses or an individual sitting at home desiring to maintain anonymity while e-shopping, the concerns about privacy on the Internet are pervasive and remain unanswered.

As a result of all the technological advances, individuals and entities around the nation and across the globe are organizing efforts to understand and generate some kind of context in which to protect privacy. Governments are struggling to identify their role in this new environment, businesses are under pressure to be aware of certain limitations and individuals are rushing to maintain their protections. As a result, we have a dynamic combination of governmental solutions, business solutions, industry solutions, advocate solutions and individual user solutions. It is difficult to make sense of these different efforts to solve a common problem and even more difficult to combine them for a focused solution. What's more, the future for protection of privacy on the Internet is completely uncharted and reveals an unwritten chapter in this nation's history. One thing is certain; the various constituencies that make up the Internet are all pushing toward new technologies and rules that provide greater control over information and privacy.

The following discussion takes a close look at DoubleClick Inc. and how they have experienced conflict and legal battles as they have apparently attempted to push the limits on an individual's right to privacy. In order to gain a better perspective on these issues, the discussion, then, continues by analyzing specific legal, technological and societal issues and giving specific recommendations and solutions for the future of "right to privacy" issues on the Internet.

THE CASE OF "DOUBLECLICK, INC."

Summary of DoubleClick Legal Actions

DoubleClick, a leading provider of comprehensive Internet advertising solutions for marketers, was incorporated as a Delaware corporation on January 23, 1996. Currently the company maintains over 30 offices globally with 1,800 employees and over 7000 customers. Recently DoubleClick also acquired Abacus Direct, the country's largest catalog database firm. The new organization combined technology, media and data expertise and used it to develop a centralized planning, execution, control, tracking and reporting system for online media campaigns. However there were growing concerns

about the manner in which consumer privacy issues were being addressed. On February 10, 2000, a complaint against DoubleClick was filed with the Federal Trade Commission (FTC) by the Electronic Privacy Information Center (EPIC).

EPIC's complaint alleged that with the merger of DoubleClick and Abacus Direct and the subsequent consolidation of their two databases, there were concerns and possible violation of the companies' assurances that the information it collects on Internet users would remain anonymous. This amounted to the data collection being unfair and deceptive. (EPIC, 2000a). EPIC also claimed that DoubleClick had failed to follow its revised privacy policy, which EPIC felt was also unfair. The allegations center around a practice known as "online profiling." DoubleClick is alleged to be tracking the online activities of Internet users by devices known as "cookies" and combining surfing records with detailed personal profiles contained in a national marketing database. In their complaint EPIC asked for relief in destruction of all records wrongfully obtained, assessment of civil penalties for the behavior and injunctive relief enjoining DoubleClick from violating the Federal Trade Commission Act.

The Executive Director of EPIC states that this complaint was filed in order to test "the current state of privacy protection in the United States." (EPIC, 2000b). It is hoped that the FTC will bring accountability to those that make promises regarding privacy and then collect personal information unfairly and deceptively.

Shortly prior to EPIC filing suit with the FTC, DoubleClick was sued in California, Superior Court, Marin County, on January 27, 2000 by Hariett Judnick seeking to represent the public in the State of California. The lawsuit alleged that DoubleClick employs "sophisticated computer tracking technology, known as cookies, to identify Internet users and collect personal information without their consent as they travel around the Web." (Junnarkar, 2000). According to the lawsuit, DoubleClick has represented to the public that it was not collecting personal and identifying information and that it gives privacy interests of Internet users paramount importance. Judnick sought relief in an injunction to stop such behavior and destruction of all information wrongfully obtained without knowing consent.

On February 29, 2000 EPIC's complaint was accompanied by The Center for Democracy and Technology's (CDT) filing a Statement of Additional Facts and Grounds for Relief with the Federal Trade Commission. Their statement similarly alleged that sensitive information including "video titles, salaries, and search terms are being passed to DoubleClick." (Junnarkar, 2000). Additionally, they asked for the FTC to stop "DoubleClick and other businesses from tying individuals' names and addresses to information collected online." (Junnarkar, 2000).

In an effort to ease public concern over the complaint, on March 2, 2000, Kevin O'Connor, CEO of DoubleClick stated that, "We commit today, that until there is agreement between government and industry on privacy standards, we will not link personally identifiable information to anonymous user activity across Web sites." (Blum, 2000).

DoubleClick's Position

DoubleClick submitted a new company policy, just after the merger, stating that it plans to use the information compiled to build a database that profiles consumers. The database will include consumers' names; addresses; retail, catalog ad online purchases histories; and demographic data. Prior to this, DoubleClick's policy had been to not connect personal information with its widespread cookies. DoubleClick now feels that it's "warning" to the public is enough notice of the act. However, "Even if DoubleClick provides warnings, such warnings give no protection to many unsophisticated Web surfers," states Ira Rothken, an attorney representing Judnick (Junnarkar, 2000).

Early on in the controversy, DoubleClick stated that it had used sensitive online data on building profiles and had no plans to do so in the future. The company had also claimed that it was their policy to only merge personally identifiable information with non-personally identifiable information for profiling, after providing clear notice and choice. (Reuters, 2000a). Looking back to 1996, when the company was first formed, Kevin O'Connor is known to have stated that DoubleClick would not be connecting its database to names, addresses and the like unless it was totally "voluntary on the user's part, and used in strict confidence. We are not going to trick people or match information from other sources" (Gillmor, 2000).

When DoubleClick joined with Abacus, it acquired a database of more than 2 billion consumer catalog transactions. This gave a clear opportunity that more than 11,500 sites that belong to DoubleClick network could feed into the new database, which could correlate with personal information (Macavinta, 2000). The stance adopted by DoubleClick in year 2000 marked the complete reversal of the policy advocated by Kevin O'Connor since the company's inception. In the new environment, it was considered adequate if the consumers were told that their information will be shared with other parties and if they were given a notice and choice for opting out.

Opponent's Position

The interesting part of this argument is that privacy advocates (for example Jason Catlett, founder of Junkbusters and quoted in Macavinta, 2000) have been stressing that the marketers will turn the Internet into a gigantic data-gathering machine for junk mail, telemarketing and advertising. Since it has now become a reality, companies such as DoubleClick, with limited or no consideration towards personal privacy characterize the 'data collection machinery' as based on choice and opting out rather than opting in.

There are also problems with DoubleClick's 'opt-out' claim. First, one will need to do it for every browser used on each and every computer. Second, the notion of trusting a trading partner and establishing a social contract with an online business gets questioned. In the case of DoubleClick, the process used to collect personal information follows three steps. DoubleClick sends a cookie to a browser and gives it a unique ID number. It then sends the same ID number on to the site that knows an individuals identity. This site (or company) then sends back the data that DoubleClick needs to look up an individual in the Abacus database. This enables DoubleClick to know who the individual is. The fact that Abacus contains names, addresses and retail information on 90% of American households creates a highly likely chance that they will be able to match the information

quickly and efficiently. Much of the information on the Internet that is collected by others "is invisible to the consumer, which raises serious questions of fairness and informed consent." (EPIC, 2000a).

The act of DoubleClick really becomes disingenuous and fraudulent when the chance to opt out comes only in the form of a few lines of text placed in the privacy policies of participating Web sites. Since such policies are usually buried a few levels down, it's rare for the consumers to find out if there personal information is being collected or their identity is being established, let alone them having a chance to opt out. Clearly this is not permission, but as David Banisar deputy director of Privacy International states, it is "fraudulent on its face." (Rodger, 2000). The issue is becomes even more complex when DoubleClick refuses to divulge the names of the participating web sites in an attempt to maintain 'confidentiality of violators of privacy.'

Status of the Case

As a result of the filings with the FTC, the FTC filed its third report to Congress making specific recommendations relevant to online privacy and online profiling. While the Commission praised the efforts of the private sector for addressing the issues of online privacy, they state that the number of Web sites meeting basic standards for privacy protection are "far too low" endangering the consumer confidence in the "fast-growing, pro-consumer marketplace". The report recommends that Congress enact legislation that ensures minimum levels of privacy protection for online consumers. The FTC recommends "basic standards of practice for the collection of information online," and a requirement that "consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online" be forced to comply with the "four widely-accepted fair information practices: notice, choice, access and security." (see FTC recommendation of May 22, 2000). The FTC believes that the proposed legislation, in conjunction with self-regulation, will provide sufficient context for Internet commerce to reach its full potential. This would allow consumer confidence to blossom facilitating full participation in the Internet marketplace.

Commentary on the DoubleClick Cases

Generally when a party files a lawsuit in any given situation, it is looking for some type of monetary damages because they have been harmed. However, in rare instances, lawsuits are filed for broader reasons, *viz*. to stop a certain behavior. The lawsuits filed against DoubleClick are an example of such actions. The individuals have not been affected by any real monetary damages. They are fighting to protect their rights and generate precedent. This is the quickest way for an individual to protect their rights, albeit it is also the most expensive.

Typically, in order to change certain implementation and remedy social concerns, the legislator is petitioned by the people or by advocates for the people, to enact legislation on the issue. However, this is likely to be a long drawn out process that could take several sessions to pass, if ever even passed at all. Thus, individuals can attack certain actions of business on a constitutional basis to have the action heard immediately and receive quick resolve through the Courts. The legislature can then, later, turn around and enact legislation that follows the Court's ruling or legislation that opposes the ruling.

In the case at hand, we not only have individual actions against DoubleClick for violations of Constitutional rights, we have private consumer and citizen protection groups (i.e. the CDT and the EPIC) filing complaints with governmental agencies in an effort to influence legislation on the issue. This sends a message to Congress that there is a problem and the citizens desire to have legislation enacted for their protection. The pleas to the FTC and to the DOC have not fallen on deaf ears and those administrative governmental agencies have submitted reports to the Federal Legislative bodies to increase protection of the citizens right to privacy through proposed legislation.

In a nutshell, the process is working. It is likely that the lawsuits will bear similar fruit, but in a more timely fashion. We have already seen the statement from DoubleClick claiming that they will "await clear industry standards before" deciding the future direction of new products and that they will not be implementing a plan to associate names with other personally identifiable information and Internet user activity (see Blum, 2000).

The procedural matter is moving full steam ahead and appears to be achieving its objectives. This is yet to be seen in full from legislation and court proceedings in the future.

DISCUSSION: RIGHT TO PRIVACY AND THE INTERNET

While the procedural issues seem to be running smoothly, there are still substantive issues that need to be researched, discussed, debated and analyzed so that a efficient and effective method can be created to protect the privacy of the citizens of the United States while still allowing capitalism to flourish. The process is only the forum for approach to the substantive issues. This section presents a brief discussion of the issues that appear to be of significant relevance and must receive consideration for any legislative body to draft effective laws and for any court to issue effective rulings.

Though not approached in this discussion, nor approached in the DoubleClick actions, access to information regarding our children, our finances, and our medical history are so valuable they cannot be ignored while discussing privacy concerns. While we merely discuss Internet access to browsing habits, loosening of Privacy Laws can lead to dissemination of information regarding our most valuable private matters.

With regard to children, suffice it to say that on October 20, 1999, the United States Congress passed a law that went into effect on April 21, 2000. The Act requires that "commercial Web sites and other online services directed at children 12 and under, or which collect information regarding user's age, to provide parents with notice of their information practices and obtain parental consent prior to the collection of personal information from children." (CDT, 2000a). It also requires those sites to provide the parents with the ability to analyze and correct their information about the child. The Act is designed to protect the child's ability to speak, seek out information and publish would not be adversely affected by these pages. Whether this will be of significant help is yet to be seen.

Medical and financial records are among the most personal information that an individual possesses. The transition of the American Health Industry from "fee-for-service" health care to the dominant managed care (i.e. HMO, PPO, etc…) has generated a demand for

an "unprecedented depth and breadth of personal information" by an ever increasing number of players. (CDT, 2000b). The ability of these entities to join forces, pool information and share records has reached an unprecedented level and will only be increasing in the future. Congress has taken efforts to regulate health privacy rules in recent sessions, however failed to meet its self-imposed deadlines. The Clinton Administration imposed an initiative listing out federal privacy rules that require consumer consent before companies share medical data or detailed information about spending habits. However, this remedy is limited, as many medical providers simply require signature of consent in order to sign up with the managed health care entity.

The basic point remains that the development of the issues is in its infancy and there are a number of very pressing concerns with regard to technology and an individual's right to privacy. The issues surrounding DoubleClick and user profiling are only the tip of the iceberg. Other issues regarding Internet privacy include National Privacy and Consumer Groups, U.S. government agencies, industry groups, various publications, privacy services, technologies and databases, "snoop" technologies, online boos, articles, papers and reports, employer access to e-mail, ISP access to information and government control of full and free access. The issues pointed out below deal with general concerns and solutions that are approached in the DoubleClick case. They are all related, however, because as the door opens ever wider, more and more rights escape, even if it is all in the name of free enterprise, don't be fooled, freedom is eroded slowly.

Technological Issues

The primary dispute, as noted in the DoubleClick case, involves "user profiling." User profiling is made possible by a technology that places identification codes on user's computers and allows access to that information by other web sites. This technology is known as a "cookie." According to Netscape, "cookies" are no longer a small treat to have with milk just prior to bed. They are a mechanism that server side connections, such as CGI scripts, can use to store and retrieve information on the client side of the connection. And the addition of a client-side state significantly extends the capabilities of Web-based client/server applications.

Cookies are embedded in the HTML code that is generated by a site and flows back and forth between the server and the user's computer. The cookies are utilized in a two stage process: first, the cookie is stored on the user's computer without their consent or knowledge – the Web server then creates a specific cookie defining certain preferences of the user in a string of text stored on the user's computer in a file called the cookie list; second, the cookie is automatically transferred from the user's computer to a Web server when ever the user brings up a specific page on the Web browser – the Web browser transmits the cookie (which contains personal information) to the server, without the knowledge of the user. In order to be warned of these cookies, the Web browser must be programmed by the user to warn of the cookies, a task not commonly known to the user. It should also be noted that the warnings only ask the use whether they consent to a cookie being deposited; if the user has no frame of reference they are clue less. (Mayer-Schönberger, 1997). A current cookie may read something like this:

> The server adlink.exchange.com wishes to set a cookie that will be sent back to any server in the domain .linkexchange.com. The name and value of the cookie

> are: SAFE_COOKIE=33ee55190305260c. This cookie will persist until Tue, Nov. 09 15:59:59: 1999.

Recently the Energy Department's Computer Incident Advisory Capability (CIAC) issued a report deeming the use of cookies as being "o.k.," however they stressed concern because at times cookies may be used for tracking an individual's browsing habits, which may make a lot of people really uncomfortable. Clearly the original intent of using cookies was to assist the user as they accessed their favorite sites by storing passwords and the like. However, it is now being utilized far beyond that scope.

The technological interchange of this information between numbers of networked entities over time could easily result in a system similar to what we presently call the "Credit Bureau." Currently the three largest credit bureaus cannot verify most of the information in their databases, which are regularly used to decide whether individuals receive credit loans, mortgages and other financing. Clearly, the Internet could become tomorrow's credit report for all to see. Consider the following scenario (Cookie Central, 2000):

> …if you visited a number of sites that advertise alcohol…and you end up on a list that your insurance company purchases. The list compiled from a variety of Internet sites shows your name as someone who frequents sites that promote alcohol, or at least as someone who is a prime prospect for alcohol sales. They raise your premiums on a profile that has been built about you based upon the sites you visit on the Internet. Someone assumes this is an accurate profile…and acts upon this erroneous assumption… This scenario may never happen but the door has been opened…Just ask anyone who has been victimized by an inaccurate credit report.

The problem that we are now facing surrounds the ability of the technology to change in an instant. While we are spending so much time and effort to stop what we *know* is invading our privacy, we have not yet approached what will be developed tomorrow that will be invading our privacy. The job of the legal community in this country is to have the foresight and the knowledge to develop a system that can regulate known and unknown technologies: a task proven to be impossible. The technology in and of itself is a living and breathing thing. It is all we can do to protect ourselves from it, no matter how much it benefits us. The balance of the benefit and the protection are unfortunately, a constant battle.

Legal Issues

The United States Constitution does not explicitly utilize the word "privacy" in any of the sections traditionally referred to as the "Privacy Amendments." However, the following Constitutional Amendments provide an array of protection of privacy that throughout history has been defined over and again[1]:

---

[1] United States Constitution; including case law: Katz v. U.S., __ Sup. Ct. __, (1967); Griswald v. Connecticut, __ Sup. Ct. __, (1965); Whalen v. Roe, __ Sup. Ct. __, (1977).

First Amendment: protects the freedom of expression and association, protecting information about those with whom we associate and materials that we generate

Fourth Amendment: safeguards individuals in their persons, homes, papers and effects, from unreasonable searches and seizures; limits government intrusion into people's private lives

Fifth Amendment: grants a privilege against self-incrimination protecting the autonomy of our bodies, thought and beliefs

Ninth Amendment: pursuant to rulings by the U.S. Supreme Court, this protects the privacy of the family and reproductive lives

Fourteenth Amendment: limits state intrusions into the freedom and privacy of intimate decisions that affect our sexual, family and reproductive lives, as defined by the Supreme Court

The United States Legislature has in recent years passed a number of laws for the protection of privacy. Initiatives issued by both the administrative branches of government, such as the FTC, and the Executive Office of the President has significantly increased over the last decade. "Internet privacy" has become an official international topic on the agenda at international government round tables through out the world. What does this mean? Clearly Internet privacy is on the mind of government. The concern for the U.S. is how they balance the interests of capitalistic democratic business, yet protect the interests of the citizens as per the Constitution.

In 1973, the standard was essentially set in The *Code of Fair Information Practices*. (Berman, 2000). This Code was set forth in the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Department of Health, Education and Welfare. The Code sets forth four primary requirements for entities gathering information. Essentially, they translate into five commonly accepted standards with which even the Internet sites must comply. Unfortunately, while the number of sites meeting this standard has doubled – from 10% in 1999 to 20% in 2000 – it still falls even shorter than that as the fair information practices are largely sealed and self-regulatory by nature (Berman, 2000). The standard includes:

Notice/Awareness: Consumers should be given notice of an entity's information practices before personal information is collected from them. The decision must be an informed decision.

Choice/Consent: Choice means giving consumers options as to how any personal information collected from them may be used; specifically relating to secondary uses of the information.

Access/Participation: This refers to an individual's ability to both access data about him/herself and to contest that data's accuracy and completeness; This includes timely and inexpensive access, simple means for contesting, a means for verification and a means for correction of the data.

Integrity/Security: Collectors of data must take reasonable steps in gathering the data, such as using only reputable sources, providing consumer access to data,

destroying untimely data; this includes both managerial and technical measures to protect against loss of the data, unauthorized access to the data, destruction, or disclosure.

Enforcement/Redress: The core principles of privacy can only be effective if a mechanism is in place to enforce them. Absent the enforcement, the Code is only suggestive; thus, self-regulation, private remedies and government penalties are all necessary.

(FTC, 1998)

The problem that we are now facing is no enforcement and failure to comply with the first four requirement standards. Even a novice can tell from the description of how the "cookie" works that it violates nearly every level of the standards. The notice that is given is not "informed," there is no explanation as to how the information will be used, the user has no access to the data that is being compiled and the data is readily transferred between entities without thought of whether the user has even given consent. Clearly, the legislature must enact enforcement measures to combat the blatant disregard for privacy in this technology. Every area of this technology violates an individual's right to privacy. It took the Federal government over a decade to enact laws governing the Credit Bureau's actions and they have still run amuck. It is hard to say if they will ever be able to get a handle on the infringement of rights on the Internet.

Solutions to Consider

Technological

There are a number of ways to combat the cookie through technological advances in the browsers. For advanced users, there is a new Platform for Privacy Preferences Project (P3P) recently developed by the World Wide Web Consortium (W3). On June 21, 2000, certain major Internet companies offered a first look at this platform (W3C, 2000). Essentially this platform provides an industry standard and a simple automated way for users to gain more control over the use of personal information on Web sites. The platform is a standardized set of multiple-choice questions covering all major aspects of Web sites privacy policies. The browser will then take a snapshot of the information on the Web site and compare it to the users information on their computer to better inform the user of the sites intentions. The industry is actively trying to find some sense to self-regulation through development of this technology.

Legal

Federal and State Legislatures are currently working on a number of bills in an effort to solve the problem. The discussion of the issues that must be considered has not even been fully formulated. However, because of the public's outcry for protection of privacy, the Legislators move forward and instead generate piece-meal bills that are hard to pass and difficult to implement as law, not to mention the fact that they largely cater to special interest groups that sponsor the legislation. A solution through this channel will be cumbersome, expensive, slow to formulate and most likely be completely ineffective.

Self Regulation

It may indeed take a very long time for the Legislature to formulate an effective privacy strategy. Hence self-regulation by individuals using the Internet may be an option. Infringement of privacy could be avoided by considering the following suggestions (CDT, 2000a):

- Look for the Privacy Policies and Web assurance seals on the Web sites
- Utilize a separate e-mail account for personal e-mail. It should not be the same as work email
- Teach children that giving out personal information online is like talking to strangers
- Clear your memory cache after browsing
- Make sure that online forms are secure
- Reject unnecessary cookies (place your browser on warn)
- Use anonymous re-mailers
- Encrypt your e-mail
- Use anonymizers while browsing
- Opt-out of third party information sharing

Of course, this does not mean that one would have all problems solved. Even Internet businesses should proactively consider the following issues, without totally excluding their ability to know who visits their sites:

- Sites should display Privacy Policies in conspicuous places and they should be stated simply
- Give the user a choice by offering a clearly written, prominently displayed opt-out box, without any of the usual "trickery-type" language
- Allow the user to inspect the record data at their whim to check for accuracy

Finally, enforcement is a must. Whether by a self-imposed monitoring authority joined by all Web sites or whether government imposed, there must be accountability for those that utilize deceptive practices and illegally track users.

CONCLUSION

Privacy on the Internet has emerged as a significant issue. Because of the technological advances, the issue of privacy goes beyond the relatively straightforward issues of seeking consent and giving choice to opt in or opt out. This chapter has brought to the fore some of the privacy concerns related to Internet commerce as evidenced by the DoubleClick case. Clearly there are ethical issues related with the use of technology and marketers in the information age need to give due consideration to various aspects of social responsibility. An ability to collect personal data and relate it to another piece of data collected with a different intent does not necessarily account for an ethical action. As

has been suggested in this chapter, good laws coupled with technological means to forewarn consumers and uniform third part assurances would go a long way in curbing the invasion of privacy in the information age.

REFERENCES

Berman, J (2000) "The Federal Trade Commission's Report to Congress – 'Privacy Online: Fair Information Practices In The Marketplace,'" CDT's Testimony, Speeches and Filings, May 25, Available at http://www.cdt.org/testimony/000525berman.shtml. Accessed November 30, 2000.

Blum, J, (2000) "Statement From Kevin O'Connor, CEO of DoubleClick," Company Press Release, Business Wire, New York, March 2, pg. 1

Center for Democracy and Technology (2000), News Web Site, http://www.cdt.org/privacy/issues/profiling.html Accessed November 30, 2000.

Cookie Central (2000), "Cookies and Internet Privacy," Internet Privacy, November 11, 2000, Available at http://www.cookiecentral.com/ccstory/cc3.htm. Accessed November 30, 2000.

Electronic Privacy Information Center (2000a), "EPIC Files FTC Complaint Against DoubleClick, Alleges 'Deceptive and Unfair Trade Practices' in Online Data Collection," Electronic Privacy Information Center February 10 News Release, Available at http://www.epic.org/privacy/internet/ftc/DCLK_comp_pr.html. Accessed November 30, 2000.

Electronic Privacy Information Center (2000b), "The Cookies Page". Available at http://www.epic.org/privacy/internet/cookies. Accessed November 30, 2000.

Federal Trade Commission (2000), "Statement of Chairman Pitofsky, Privacy Online: Fair Information Practices in the Electronic Marketplace" May 22. Available at http://www.ftc.gov/reports/privacy2000/pitofskystmtonlineprivacy.htm. Accessed November 30, 2000.

Federal Trade Commission (1998), "Privacy Online: A Report To Congress," Section III. Fair Information Practices Principles, June 1998, Available at http://www.ftc.gov/reports/privacy3/toc.htm. Accessed on November 30, 2000.

Gillmor, D (2000) "DoubleClick does double take on Web privacy," SiliconValley.com News, January 27. Available at http://www0.mercurycenter.com/svtech/columns/gillmor/docs/dg012800.htm. Accessed on November 30, 2000.

Junnarkar, S, (2000) "DoubleClick accused of unlawful consumer data use," CNET News.com, January 28. Available at http://news.cnet.com/news/0-1005-200-1534533.html. Accessed November 30, 2000.

Macavinta, C (2000), "Privacy fears raised by DoubleClick database plans," CNET News.com, January 25. Available at http://news.cnet.com/news/0-1005-200-1531929.html?dtn.head. Accessed November 30, 2000.

Mayer-Schönberger, V (1997) "The Internet and Privacy Legislation: Cookies for a Treat?" West Virginia Journal of Law and Technology 1:1 Available at http://www.wvu.edu/~wvjolt/Arch/Mayer/Mayer.htm. Accessed November 30, 2000.

Reuters (2000a), "DoubleClick defends data practices," ZDNET News, February 17, Available at http://www.zdnet.com/zdnn/stories/news/0,4586,2439228,00,html?chkpt=zdnntop. Accessed November 30, 2000.

Reuters (2000b), "DoubleClick sued over privacy," ZDNET News, January 28. Available at http://www.zdnet.com/zdnn/stories/news/0,4586,2429053,00.html?chkpt=zdnnrla. Accessed November 30, 2000.

Rodger, W, "Activists charge DoubleClick double cross," USA Today.com, June 7, Available at http://www.usatoday.com/life/cyber/tech/cth211.htm. Accessed on November 30, 2000.

W3C (2000) "Platform for Privacy Preferences (P3P) Project," June, Available at http://www.w3.org/P3P/. Accessed November 30, 2000.