
Ethan Hayward

Follow this and additional works at: https://via.library.depaul.edu/jatip

Recommended Citation
Available at: https://via.library.depaul.edu/jatip/vol11/iss1/8

This Legislative Updates is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Journal of Art, Technology & Intellectual Property Law by an authorized editor of Via Sapientiae. For more information, please contact digitalservices@depaul.edu.
LEGISLATIVE UPDATES

THE FEDERAL GOVERNMENT AS COOKIE INSPECTOR: THE CONSUMER PRIVACY PROTECTION ACT OF 2000

I. INTRODUCTION

Nearly every Internet user has at some point in time received a commercial email message she does not remember soliciting, and has most likely wondered how the sender was able to ascertain her email address, much less her potential interest in the exciting offer contained therein. Even more common is the banner advertisement that appears on commercial web sites, that seems to know the exact age, gender, and income bracket of its target. For example, subscription offers to magazines such as Details and Maxim will appear to young adult male surfers, while links to Internet personal ads will appear to known single users. The explanation is simple: The advertisers know who you are and where you are. Internet advertisers and e-commerce web sites employ a technology known as “cookies”\(^1\) to track exactly when and where users log on to browsers in general and to certain web sites in particular. Web advertisers often use a cookie’s transmission pattern to build a user profile based on the type of

---

\(^1\) Cookies work fairly simply. Web site proprietors – or more often, third party Internet advertising agents – will transmit a text file to a user’s personal computer when that user is connected to a particular site. The file contains an identification number that is matched with a user’s Internet address, and the number is transmitted back to its original sender with each subsequent visit by the particular user. These files are sent and retrieved most often without the user’s knowledge, and more importantly, without the user’s consent. See Will Rodger, *Activists Charge DoubleClick Double Cross: Web Users Have Lost Privacy with the Drop of a Cookie, They Say*, USATODAY.com Tech Report, June 7, 2000 (visited Oct. 18, 2000) <http://www.usatoday.com/life/cyber/tech/cth211.com>.

227
Web sites the user visits most frequently, and will use that profile to target banner ads and email to that user every time she logs on.\(^2\)

As with any rapidly advancing technology, the potential for abuse exists.\(^3\) Recent events in the business world have enabled companies to match on-line profiles with personally identifying information such as names and addresses.\(^4\) The most conspicuous example is the November 1999 merger of DoubleClick, the world’s most prominent Internet advertising firm, with Abacus Direct, the keeper of the country’s largest database of mail-order customers.\(^5\) In January 2000, DoubleClick announced it would begin associating users’ names and addresses with data compiled through its on-line tracking program.\(^6\) According to a survey

\(\footnotesize{2\text{ Id.}}\)

\(\footnotesize{3\text{ A complaint filed by Michigan Attorney General Jennifer Granholm alleges that one Internet advertiser compiles and sells its cookie-aided profiles to third parties without users’ knowledge or consent, and that such a practice amounts to “little more than a secret, cyber wiretap.” State of Michigan Attorney General Press Release, Feb. 17, 2000 (visited March 1, 2000) <http://167.240.254.37/AGWebSite/press_release/pr10164.htm>.}}\)

\(\footnotesize{4\text{ A complaint filed with the Federal Trade Commission against DoubleClick, Inc. by the Electronic Privacy Information Center (EPIC) claims that DoubleClick’s recent acquisition of Abacus Direct Corp. (a national catalog company with a massive database of detailed contact information for numerous subscribers) has enabled the company to combine its tracking data with personally identifiable information. EPIC FTC Complaint (visited Oct. 27, 2000) <http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf>. The FTC recently announced that it would not continue its investigation, acknowledging that DoubleClick has not begun to merge its online and offline data. Bob Tedeschi, DoubleClick Seeks Ways to Protect Users’ Anonymity, NY TIMES, Jan. 29, 2001 (visited Jan. 31, 2001) <http://www.nytimes.com/2001/01/29/technology/29ECOMMERCE.html>. However, the FTC did indicate that the close of the investigation was “not to be construed as a determination that a violation may not have occurred. Letter from Joel Winston, FTC Acting Associate Director, to Christine Varney, DoubleClick Counsel, dated Jan. 22, 2001.}}\)

\(\footnotesize{5\text{ Rodger, Activists Charge DoubleClick Double Cross, USATODAY.com Tech Report, June 7, 2000 <http://www.usatoday.com/life/cyber/tech/cht2111.com>.}}\)

conducted by Business Week in March 2000, 82% of Americans fear that such practices could lead to their on-line activities being associated with even more private information, such as credit data and medical history. According to the same survey, 57% of those polled favored legislation regulating how personal information is collected and used by e-marketers.

In 1998, Congress enacted the Children’s Online Privacy Protection Act, which makes it illegal for web site operators to collect personal information from children under the age of thirteen without express notice to and consent of a parent. The European Union has enacted a similar law that requires businesses to collect private data from European citizens only for clearly stated purposes and which forbids data disclosure to third parties without consumer permission. To date, no such legal restrictions exist as to the gathering and use of personal data from adults in the United States. Several recent resolutions by Congress have proposed to remedy this situation. The most comprehensive measure introduced is the Consumer Privacy Protection Act of 2000, sponsored by Senator Ernest “Fritz” Hollings.

II. BACKGROUND

A. Self-Regulatory Measures

In the Information Age, basic information as to a person’s whereabouts and preferences has become an extremely valuable

---

8 ld.
Businesses today keep detailed logs of consumers’ transactions, and target sales of particular goods or services to individual consumers based on their past purchases. Some businesses in turn sell or rent their accumulated information to other marketers. This simple practice was projected to generate $3 billion in revenue as early as 1994. Some e-commerce retailers regularly and admittedly give or sell customer information to other online partners, making sales contingent on consumers’ consent to the practice. Some Internet search engines have for years recorded their users’ search terms and built profiles so they may offer customized advertising and command higher rates from advertisers seeking particular demographics. Computer hardware manufacturers attempted to facilitate user identification in 1999 when Intel announced that its latest model processor chip would transmit an individual serial number over network connections. The signal would alert web marketers to a user’s presence as soon as a connection is established, and possibly allow the marketers to discover the identity of the person to whom the hardware was registered. Web marketers often engage in a practice known as “data mining,” employing software to search firms’ databases for information that would prove useful to their own store of knowledge. Not surprisingly, most of this activity occurs undetected by the average web surfer.

12 Jon Healey, The Promises of New Technologies Also Pose a Threat to Personal Privacy, CONGRESSIONAL QUARTERLY WKLY RPT, May 14, 1994, at 42.
13 Id.
14 Id.
16 Id.
18 Id.
In an effort to avoid outright regulation, the industry has offered to police itself, both individually and collectively.\footnote{DoubleClick, Inc. Form 10-K/A (Amendment No. 2) for Calendar Year Ended Dec. 31, 1998.} DoubleClick has acknowledged that it plans to use statistical models assembled through the use of its cookies to deliver advertising messages to online consumers identified by Abacus Online, its new subsidiary.\footnote{Most web retailers and web-based companies display individual privacy policies on their sites, setting out, in detail, what kind and how much personal information the company intends to collect, what the information will be used for, and consumers’ options for retrieving, accessing, and retracting information obtained from them. Other companies rely on specialty organizations to certify their policies through “privacy seal” programs. Examples include the Better Business Bureau Online \(<\text{www.bbonline.org}\>\) and Trust-E \(<\text{www.truste.org}\>\). These programs evaluate a site’s privacy policy for its adherence to privacy standards prescribed by U.S. and international law. Once it has been determined the site’s policy is in compliance, the program will display a “privacy seal” on the site’s main page to certify that the site’s policy meets minimum legal standards. The seal organizations also serve as intermediaries in privacy disputes, allowing consumers to report possible violations and working with the certified company to ensure that its policies are not violated.} The company also asserts through its privacy policy that it will collect personally identifiable information only with clear notice to and consent of users, and that information in the resulting database will not be disclosed to other merchants.\footnote{Id.} Finally, DoubleClick has vowed not to associate any personally identifiable information it possesses with any identifiable medical, financial, or sexual preference information of individual users.\footnote{Id.}

However, DoubleClick’s business model is that of a vast network of web operators who deal with individual users directly.\footnote{EPIC FTC complaint \(<\text{http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf}\>\).} These other operators within the network could

patterns in seemingly unrelated data. In a commercial setting, the software is most often used by retail companies to find customers with common interests. \cite{webopedia}
conceivably synchronize their own cookie technology with that of DoubleClick, allowing both parties to learn the identity of a consumer and to pass the resulting information on to other network participants almost instantaneously.26 Such an arrangement could cause a user’s personal information to be shared with several web marketers when the user intended to disclose the information to only one.27 Thus, the user would rarely be afforded an opportunity to receive notice and give consent to the collection and use of her personal information in the DoubleClick/Abacus network.28 Furthermore, DoubleClick has made no mention of the information already possessed by Abacus at the time of the merger this past June of 2000.29 It only offers access and opt-out measures to users who voluntarily provide personal information via its network.30 There is no mention of a means by which consumers may retract information acquired through DoubleClick’s co-op partners.31 Such a process would require each individual partner (who number in the thousands) to provide opt-out measures. The logistical impossibility of controlling the flow of personal information and the inability to enforce the opt-out provision renders DoubleClick’s privacy policy all but ineffective. Privacy advocates have compared such measures by DoubleClick to an innkeeper installing do-not-disturb signs instead of locks on guest room doors.32

Commercial web publishers have initiated several programs to try to establish a more comprehensive and uniform means of providing Internet users with notice, consent, access, and security as prerequisites for collection of personal information.33 These

27 Id.
29 See supra note 22.
30 Id.
31 Id.
32 See supra note 26.
33 See supra note 21.
programs take the form of privacy seals, which are placed on participating web sites to assure users of compliance with the privacy policy standards set forth by the sponsoring organizations.\(^{34}\) The most notable examples of such initiatives are TRUSTe, Better Business Bureau Online, and SecureAssure,\(^ {35}\) who affix their seals of approval to sites that have met their privacy standards, in exchange for reasonable fee.

The main criticism of such programs is that they have been established and are funded by the very parties they claim to oversee; a case of the fox guarding the hen-house.\(^ {36}\) Others claim that the seal programs lack any real enforcement mechanisms.\(^ {37}\) The most severe penalty they may impose is withdrawal of a seal, which rarely occurs even for flagrant violations.\(^ {38}\) Several e-tailers have been found to violate their seal-certified promises not to share customer information with third parties, without the seal program ever knowing about it.\(^ {39}\) Apparently, whistleblowers are necessary in order for privacy violations to come to the attention of industry regulators.

In one instance, TRUSTe did report a serious violation to the Federal Trade Commission, which resulted in the FTC filing a complaint against the participant.\(^ {40}\) In that case, Toysmart.com declared bankruptcy and sought to liquidate its assets. Among these assets was its customer database. In obtaining the information contained therein, Toysmart.com assured its customers their information would not be shared with third parties,

\[\text{34 Id.}\]
\[\text{35 Id.}\]
\[\text{36 Berst, <http://www.zdnet.com/filters/printerfriendly/0,6061,2641042-10,00.html>}.\]
\[\text{38 Id.}\]
\[\text{40 Stephanie Stoughton, FTC Sues Toysmart.com to Halt Data Sale; Bankrupt E-Retailer Made Privacy Vow to Customers, BOSTON GLOBE, July 11, 2000, at E2.}\]
a practice that had been certified by TRUSTe. Upon declaring bankruptcy, Toysmart.com did in fact offer the database for sale. TRUSTe learned of the situation through an anonymous tip and reported it to the FTC, which subsequently filed a complaint. The two sides reached a settlement agreement in July 2000, which would allow Toysmart.com to sell the data under certain circumstances. The decree was met with opposition by privacy advocates and attorneys general, who claim that the customers should be notified and have the option to have their information deleted from the database. Subsequently, the parties agreed to a subsidized destruction of the customer database.

This situation leaves one to wonder how effective industry self-regulation can truly be, given that the actual authority to sanction privacy violations ultimately lies with the government. In effect, the government, through the FTC, has been asked by TRUSTe to enforce a TRUSTe policy violated by a third party. Having one entity look to another to promulgate privacy policies and subsequently having that second entity look to the government to enforce those policies appears altogether convoluted and inefficient. When a system of self-policing apparently requires enforcement by a middle man, its effectiveness is difficult to discern. Further complicating the situation is the fact that many online retailers “outsource” their information processing functions to specialists in that area. Such arrangements beg the question as

---

42 Stoughton, Judge Declines to Rule on Toysmart Database; Stalls Sales of Customer Information, BOSTON GLOBE, Aug. 18, 2000, at C2.
43 Id.
44 Id.
47 Toys R Us was recently named in a New Jersey class-action lawsuit for outsourcing the data processing done through its web site to Coremetrics, a data processing specialist, after stating in its privacy policy that the retailer would not share customers’ personal information with third parties without customer.
to which entities actually constitute third parties and which entities are bound by and responsible for the enforcement of the operator’s privacy policy.

Further complications arise from the fact that sites bearing the same seal may have substantially different privacy policies and methods of enforcement.\(^48\) Thus similar violations by different companies may incur differing penalties or none at all.\(^49\) Another possibility would be that one seal program may sanction a certain practice while another program allows it to go on unabated.\(^50\)

Finally, skeptics maintain that an inherent conflict of interest exists in entrusting industry-funded seal programs to police the habits of their benefactors.\(^51\) The entire concept of privacy seal certification between private companies has been labeled by Junkbusters president Jason Catlett as “a public relations and lobbying effort” whose “main aim is to stave off legislation.”\(^52\)

\textbf{B Consumer Action}

Some measures of protection are accessible to the computer savvy consumer who wishes to maintain her privacy. Unfortunately, location and implementation of such measures entail varying amounts of time, effort, and money, luxuries which are not always available to the average web surfer.\(^53\)

Anonymizer is a web-based company that provides privacy protection software to users over the Internet.\(^54\) These programs

---


49 Id.

50 Id.

51 Id.


are downloadable and most often operate as plug-ins to web browser applications.\textsuperscript{55} The company offers a free service that hides an individual user's IP address and removes cookies and other identifying programs from a browser's cache while it is operating.\textsuperscript{56}

Anonymizer offers other protections on a fee per service basis. Among these is a program called Safe Cookies which is used to encrypt and conceal cookies sent to a user's hard drive via remote web sites.\textsuperscript{57} Most web browsing applications include an option to disable cookies, which allows users to refuse to accept cookies sent to their hard drives from remote computers. However, some of the more popular commercial web sites and portals require that cookies be enabled and will deny access to users who refuse to comply.\textsuperscript{58} Smart Cookies allows users to access these sites by re-routing cookies to Anonymizer servers, which re-formats and encrypts the cookie so that they may not be read while a user is online and disappear when a user quits her browser.\textsuperscript{59}

Due to the varying practices and technology used in web communications, programs like Safe Cookies do not always function with some of the more frequently visited web sites and portals. These programs and their ancillary equipment do not always possess the speed and capacity necessary to intercept and reformulate the varying numbers and sizes of cookies transmitted by web servers.\textsuperscript{60} As a result, users may experience very slow download speeds on cookie-required sites or be denied access to them altogether.\textsuperscript{61}

Another device that allows users to block cookies and other uninvited communications is known as a proxy. A proxy is essentially a third computer enlisted to filter communications from

\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{58} Id.
\textsuperscript{59} Id.
\textsuperscript{60} Id.
\textsuperscript{61} Id.
one computer to another. Anonymizer is an example of one such service. However, some of the more prominent providers of Internet content, namely Microsoft, will not validate users whose IP addresses the provider is not able identify and maintain. Hence, while proxies are effective in maintaining user anonymity, they often hinder users in cases where identification is prerequisite to accessing necessary web content.

Perhaps the most comprehensive technological privacy control measure proposed to date is the Platform for Privacy Preferences Project (P3P). P3P is basically a set of guidelines for web-browsing software designed to provide users with a clearer understanding of how personal information will be used by particular web sites. The platform also enables web site operators to explain their privacy policies to users directly through the browsing software: Once a user attempts to access a particular site using P3P, the user will receive a message conveying that site's practices regarding personal information. The user then may decide whether or not to proceed to the site.

While P3P does have the potential to increase greatly consumer awareness as to the information practices of leading web operators, the platform was only recently introduced and as such is not yet in wide use. Furthermore, no authority exists to mandate its use. Finally, while P3P may indeed serve to make consumers more aware of the risks they incur when visiting certain sites, it may ultimately be limiting in that consumers who wish to protect their personal information will be deterred from

64 Id.
65 Id.
66 Id.
68 Id.
visiting sites they would otherwise access were they given an option of doing so without divulging their information.

C. Federal Legislation

Because the vast majority of web content providers and e-tailers have proven neither ready nor willing to implement an industry-wide and comprehensive means of self-regulation on privacy matters, many privacy activists, private consumers, and even the Federal Trade Commission have called for federal laws to guarantee privacy protection online. Furthermore, the passage of the EU Privacy Directive has inhibited the expansion of some e-marketers whose privacy policies do not comply with European law. This situation highlights the need for a comprehensive U.S. law that would set minimum standards for consumer privacy on the Internet and clarify jurisdictional discrepancies. Such a law does exist in the Children’s Online Privacy Protection Act (COPPA), which regulates when and how much personal information may be gathered from children under the age of thirteen. However, no such protection is currently available for adult users.

1. Children's Online Privacy Protection Act

Enacted in October 1998, the Children's Online Privacy Protection Act has been met with relief on the part of parents and confusion and sometimes frustration on the part of web operators.\textsuperscript{74} The Act (COPPA) requires operators of web sites directed to children and operators with actual knowledge that they are collecting personal information from children to provide notice on the web site of what information is collected and how it is used.\textsuperscript{75} COPPA also requires that operators obtain verifiable parental consent before collecting or using such information.\textsuperscript{76} Further, the Act requires that web site operators afford parents the opportunity to review any information that sites have collected from their children and to prohibit further use or maintenance of children's information, a practice known in the industry as an "opt-out."\textsuperscript{77} Finally, COPPA requires operators to maintain reasonable procedures to protect the confidentiality, security, and integrity of the information they collect from children.\textsuperscript{78} The Federal Trade Commission issued its final rule on COPPA in April 2000 and is the agency authorized to bring enforcement actions for violations of COPPA provisions.\textsuperscript{79}

Compliance with COPPA has been met with resistance by many and by abject surprise by some. In October 2000, observers discovered that web sites operated by the federal government were soliciting personal information from children without requiring parental consent beforehand.\textsuperscript{80} For example, a White House site invited children submit their names, ages, and addresses in email messages to the President.\textsuperscript{81} Sites operated by the EPA and NASA

\textsuperscript{75} Id. at (b)(1)(A)(i).
\textsuperscript{76} Id. at (b)(1)(A)(ii).
\textsuperscript{77} Id. at (b)(1)(B)(ii) and (iii).
\textsuperscript{78} Id. at (b)(1)(D).
\textsuperscript{79} 16 C.F.R. § 312 (2000).
\textsuperscript{81} Id.
also collected identifying information from children who submit art work as content for the sites.\textsuperscript{82} As enacted, COPPA is not applicable to government sites, but a recent order from the Office of Management and Budget mandates that federal agencies comply with its provisions.\textsuperscript{83}

Such phenomena have prompted indignation from operators of private children’s sites, some of whom have had to scale back features such as email, chat rooms, and electronic bulletin boards because of the high costs of obtaining and verifying parental consent.\textsuperscript{84} Hence the law seems to hit small scale operators much harder than those with more ample resources. Also, the law could be difficult to enforce against operators that are known to deal with both adults and children, in that such operators would be required to differentiate the ages of users in order to be ensure compliance.\textsuperscript{85}

2. Electronic Communications Privacy Act

The Electronic Communications Privacy Act was passed in 1986 as an amendment to the Federal Wiretap Act.\textsuperscript{86} With regard to personal information, the Act prohibits electronic service providers from knowingly disclosing to any third party the contents of stored communications.\textsuperscript{87} However, the law contains an exception for divulging the contents of such communications to an addressee or intended recipient.\textsuperscript{88} When users provide personal information to web operators, the operators could be construed as the intended recipients and would be allowed to do with the information what they please.\textsuperscript{89} As such, this law seems to have little to no effect on

\begin{footnotesize}
\begin{enumerate}
\item Id.\textsuperscript{82}
\item Id.\textsuperscript{83}
\item Id.\textsuperscript{84}
\item Id.\textsuperscript{85}
\item 18 U.S.C. § 2701 (2000).\textsuperscript{86}
\item 18 U.S.C. § 2702 (2000).\textsuperscript{87}
\item Id. at (b)(1).\textsuperscript{88}
\item 18 U.S.C. § 2702 (b)(5). Subsection (b)(5) provides an exception for any communication “as may be necessarily incident to the rendition of the service or
\end{enumerate}
\end{footnotesize}
the information voluntarily provided to web operators, who may in turn transfer personal data to third parties as intended recipients themselves.90

3. The Gramm-Leach-Bliley Act

Passed as the Financial Services Modernization Act, the Gramm-Leach-Bliley Act was enacted in 1999 as means to facilitate affiliation among banks, securities firms, and insurance companies, principally by sharing information.91 Title V of the Act requires that financial institutions disclose their privacy policies to affiliates and third parties and that they provide consumers with the opportunity to opt-out of sharing their information with nonaffiliated third parties.92 On its face, this measure could be seen to regulate the privacy practices of financial institutions that do business online.93 Again, however, the legislation would apply only to a limited number of web operators and leave many others to disregard any measure of privacy protection.94

90 18 U.S.C. § 2702 (b)(4). Subsection (b)(4) allows communications of personal information “to a person employed or authorized or whose facilities are used to forward such communication to its destination.” This exception could easily apply to third parties to whom web operators outsource their data processing functions.
92 Id. at Sec. 502.
4. The Fair Credit Reporting Act

Passed in 1970, the Fair Credit Reporting Act (FCRA) permits information sharing within a corporate family of information relating to transactions between financial affiliates and consumers.\(^{95}\) Under the Act, affiliates may share any information that bears on a consumer’s credit-worthiness provided they follow a notice and opt-out procedure.\(^{96}\) FCRA also requires that consumers be able to access reports kept by credit institutions to ensure their accuracy and completeness.\(^{97}\) Again, though, this law could have limited scope given the vast array of content and service providers on the Internet.\(^{98}\)

D. State Legislation

In the wake of the Gramm-Leach-Bliley Act, several states have proposed similar legislation, most protecting consumer privacy with respect to financial institutions and some extending protection to a much larger commercial context.\(^{99}\) States focusing their efforts on the latter situation include Arizona, Hawaii, Illinois, and New Hampshire.\(^{100}\)

The Arizona bill would restrict the collection and disclosure of personal information provided by consumers to “information custodians,” broadly defined as all entities that maintain and share

---

96 Id. at (b).
97 Id.
98 See supra note 94. The terms “affiliates” and “business partners” are open to broad interpretation. Any number of web operators and other third parties can and could qualify as business partners of vast credit providers. Kempler and Woody, Living with the Gramm-Leach-Bliley Act <http://www.insurelegal.com/livingwith031500.html>.
99 Id.
100 Id.
personal data with others. The bill requires these entities to establish and disclose a privacy policy on the entities’ web sites and to allow consumers an option not to have their information shared. The bill would allow aggrieved parties to recover $500 per violation from entities who violate their policies, with treble damages awarded in cases where the violations are found to be willful.

The Hawaii bill prohibits private enterprises from disclosing to third parties any personal data collected about an individual unless the individual gives express consent to have the information released. The bill mandates that private entities collecting personal information provide notice to consumers explaining the purpose of the collection, the entities’ planned use of such data, the types of persons in the enterprise who will have access to the data, where the data will be stored, and consumers’ rights to access and correct the information collected. Intentional violations of the bill’s provisions would be treated as misdemeanors in criminal cases and could incur civil damages ranging from $1,000 to $5,000 per violation.

An Illinois proposal prohibits state agencies and officials from selling information regarding Illinois citizens to any entity for commercial solicitation purposes. Commercial solicitation purposes under the bill include contacting individuals in order to advertise, offering products or services for sale, or identifying potential employees. The bill requires commercial purchasers of state databases to disclose the proposed use of the intended purchase. Failures to disclose the above-mentioned purposes or

---

102 Id.
103 Id.
104 H.R. 1232, 20th Leg. (Haw. 1999).
105 Id.
106 Id.
108 Id.
109 Id.
misrepresentations in such agreements are punishable as petty offenses.\textsuperscript{110}

In New Hampshire, legislators have proposed creating an executive state office on privacy.\textsuperscript{111} Under the bill the director of said office would assure compliance with other provisions, mainly the requirement that the state not disclose personal information to private entities without the individual's written consent.\textsuperscript{112} Individuals may sue the state for violations of this provision and be awarded compensatory damages as well as special damages in the amount of $1,000 for each violation. The bill also provides injunctive relief in lieu of monetary penalties.\textsuperscript{113}

\textit{E. Litigation}

Because of the ever-changing nature of communication technology and the varying applicability of privacy principles to the numerous different means of communication, much litigation has arisen concerning businesses' use of customer information for marketing purposes. In \textit{U.S. West Inc. v. Federal Communications Commission},\textsuperscript{114} the court of appeals for the Tenth Circuit heard a petition for review of an FCC rule which restricted the use and disclosure of and access to customer proprietary network information (CPNI).\textsuperscript{115} The rule was initiated to implement Section 222 of the Telecommunications Act of 1996, which requires that telecommunications carriers only disclose individually identifiable CPNI with the approval of the customer.\textsuperscript{116} The statute also defined CPNI as information relating to the quantity, type, and amount of use of a communications service that is made available to the carrier solely by virtue of the

\begin{itemize}
\item \textsuperscript{110} Id.
\item \textsuperscript{111} H.R. 1612-FN, 156th Gen. Ct. (N.H. 2000).
\item \textsuperscript{112} Id.
\item \textsuperscript{113} Id.
\item \textsuperscript{114} U.S. West Inc. v. Federal Communications Commission, 182 F.3d 1224 (10th Cir. 1999).
\item \textsuperscript{115} Id. at 1228
\item \textsuperscript{116} 47 U.S.C. § 222(c)(1) (2000).
\end{itemize}
carrier-customer relationship.\textsuperscript{117} In essence, CPNI is information regarding when, where, and to whom customers place calls, and as such the court afforded it a high level of privacy protection.\textsuperscript{118} In this case, the petitioner, a telecommunications provider, challenged the FCC regulation, claiming it was arbitrary and capricious and violated the First Amendment protection afforded commercial speech.\textsuperscript{119} In particular, U.S. West objected to the FCC’s requirement that carriers employ an opt-in approach when seeking and obtaining customer approval to share CPNI with affiliated and non-affiliated businesses.\textsuperscript{119} The opt-in approach entails obtaining express approval from a customer by written, oral, or electronic means before using or disclosing that customer’s information. The court, applying the \textit{Central Hudson} test,\textsuperscript{120} agreed with the petitioner and vacated the FCC order, holding that sharing of CPNI between carriers constituted lawful and non-misleading commercial speech, was related solely to the economic interests of the speaker and its audience, and that the regulation implicated carriers’ rights to free and unfettered commercial speech.\textsuperscript{121}

Specifically, the court found that, despite the assumption that customer calling patterns are a private matter and restricting access to them could constitute a substantial government interest, the FCC’s approach to obtaining customer approval did not directly and materially advance this interest and was not as narrowly tailored as it should have been.\textsuperscript{122} The court sided with U.S. West, who advocated an opt-out approach as a less restrictive means of

\textsuperscript{117} \textit{Id.} at § 222(f)(1)(A).
\textsuperscript{118} \textit{U.S. West}, 182 F.3d at 1229, n1.
\textsuperscript{119} 47 C.F.R. § 64.2007(b).
\textsuperscript{120} \textit{Central Hudson} Gas & Elec. Corp. v. Public Serv. Comm’n of N.Y., 447 U.S. 557 (1980). \textit{Central Hudson} holds that governments may institute regulations on commercial speech, provided it is neither misleading nor advocating illegal activity, if: (1) there is a substantial government interest at stake; (2) the regulations directly advances that government interest; and (3) the regulations are narrowly tailored and not overly restrictive in fulfilling the government interest.
\textsuperscript{121} \textit{U.S. West}, 182 F.3d 1224, 1231-1233.
\textsuperscript{122} \textit{Id.} at 1237-1239.
implementing the congressional restriction on sharing CPNI. This approach merely requires carriers to provide customers with notice of their intent to use and share CPNI for marketing purposes, and a mechanism for customers to opt-out of the proposed use.\(^\text{123}\)

The dissent employed a *Chevron* analysis\(^\text{124}\) to arrive at the conclusion that the FCC's approach was a reasonable interpretation of the statute and that it did advance the substantial state interest of protecting consumer privacy.\(^\text{125}\) Moreover, the dissent asserted that the opt-out approach did not meet the statute's requirement of informed customer consent before use of CPNI would be allowed.\(^\text{126}\)

The Eighth Circuit took a somewhat different approach to telecommunications privacy in *Van Bergen v. Minnesota*.\(^\text{127}\) In that case, the plaintiff sought to enjoin the state's enforcement of a statute regulating automatic telephone dialing-announcing devices. In particular, the law forbade the use of the devices by callers who did not have a prior business or personal relationship with the call recipient between the hours of 9:00 a.m. and 9:00 p.m.\(^\text{128}\) The plaintiff, a gubernatorial candidate, planned to use automatic caller devices to reach potential voters and provide them with a toll-free number by which they could obtain more information about his campaign.\(^\text{129}\) *Van Bergen* argued that the statute was overbroad, was content-based, and restricted access to a public forum, and was therefore in violation of the First Amendment. The court found that the law was a reasonable time, place, and manner restriction which allowed telephone solicitors a 12-hour span in

\(^{123}\) *Id.* at 1240.

\(^{124}\) *Chevron* U.S.A. Inc. v. Natural Resources Defense Council, 467 U.S. 837 (1984).\(^\text{Chevron*} \text{governs statutory construction by executive agencies and courts, and holds: (1) that legislative intent is clear when Congress has spoken directly to the precise question at issue and that courts and agencies must give effect to that intent; and (2) that when a statute is silent or ambiguous as to a given issue, the question is whether the agency's interpretation is based on a permissible construction of the statute.}\(^\text{125}\) *U.S. West*, 182 F.3d at 1246.

\(^{126}\) *Id.* at 1247.

\(^{127}\) 59 F.3d 1541 (8th Cir. 1995).

\(^{128}\) *Id.* at 1546.

\(^{129}\) *Id.*
which to ply their trade. The court also found that the regulation did not restrict automatic dialer calls based on content, but rather on the existence or non-existence of the caller’s prior relationship with the recipient; the statute allowed automatic messages from schools to students and parents as well as from employers to employees because such entities necessarily have prior relationships. The law thus passed the test for content neutrality established under *Ward v. Rock Against Racism*. The court further held that the telephone system was a private channel of communication and that the government had a substantial interest in protecting residential privacy from unsolicited and unconsented-to auto dialer calls. Finally, the court concluded that the statute was a reasonable time, place, and manner restriction on commercial speech in that it placed only a minimal burden on auto dialer callers to obtain recipient consent before sending a recorded message during restricted hours, and that it left open numerous alternative channels for speakers to reach their intended audience.

In reaching its decision, the *Van Bergen* court seemed to employ the same reasoning as that used by the dissent in *U. S. West*. Specifically, the *Van Bergen* court emphasized the recipient’s opportunity, or lack thereof, to indicate his or her desire to receive automated telephone messages. Based on this condition, the court found that the government has a substantial interest in protecting the privacy and tranquility of the home and the efficiency of the workplace from the intrusive nature of these calls. Diverging from the *U. S. West* majority holding, the *Van Bergen* court found that the regulation under review did not need to be the least restrictive means of achieving the government

---

130 *Id.* at 1549.
131 *Id.* at 1550.
132 491 U.S. 781 (1989). *Ward* holds that governments may impose reasonable restrictions on the time, place, or manner of engaging in otherwise protected speech provided that the restrictions are adequately justified and not based on the content of the regulated speech.
133 *Van Bergen*, 59 F.3d at 1553-1555.
134 *Id.* at 1555.
135 *Id.*
interest in order to meet the narrow tailoring requirement of the Central Hudson test. 136

In Conboy v. AT&T Corp., 137 the federal district court for the Southern District of New York dismissed claims against the defendant for violations of the privacy provisions of the Telecommunications Act 138 and the Fair Debt Collection Practices Act (FDCPA). 139 Plaintiffs were AT&T long distance customers and alleged that AT&T disseminated their CPNI, phone bill information, unlisted phone numbers, and billing names and addresses to its credit card division and other entities without prior consent. 140 Plaintiffs filed suit when representatives of AT&T’s credit card division repeatedly phoned plaintiffs’ unlisted number seeking information as to their daughter-in-law’s whereabouts. The calls came at all hours of the day, and one representative even revealed that he knew the plaintiffs’ unlisted personal information and the details of their calling patterns. 141 The plaintiffs claimed these calls were the direct result of AT&T’s sharing of customer information with third parties and AT&T’s failure to provide notice to customers that it engaged in such practices. 142

Plaintiffs brought suit under section 222 of the Telecommunications Act, which, as stated in the U. S. West case, restricts carriers in sharing CPNI with third parties without customer approval. 143 The court dismissed the charge for failure to state a claim, reasoning that the plaintiffs only paid a fee to their local phone carrier to keep their information unlisted and gave no such consideration to AT&T to do the same. 144 Although AT&T was alleged to have violated the Telecommunications Act, plaintiffs had no private right of action because they could not demonstrate damages. The court reasoned that because plaintiffs

136 See Id. at note 13.
137 84 F. Supp. 2d 492 (S.D.N.Y. 2000).
140 Id. at 496.
141 Id. at 497.
142 Id.
143 47 U.S.C. § 222(c)(1).
144 Conboy, 84 F. Supp. 2d at 499.
received all the services for which they paid AT&T – compliance with the Act not among them – they suffered no personal damages from AT&T's alleged noncompliance.\footnote{Id. at 499, 500.} The court also dismissed a similar claim brought under FCC regulations promulgated under the Telecommunications Act, which prevent communications service providers from disclosing the billing name and address of subscribers to third parties.\footnote{47 C.F.R. § 64.1201(c)(2).} The court found no explicit or implicit provision in the regulation allowing a private right of action for violations, and therefore barred the plaintiffs' claim.\footnote{Conboy, 84 F. Supp. 2d at 500-502.}

The plaintiffs brought another count under section 1692e(11) of the FDCPA, which mandates that debt collectors disclose in their initial communications with consumers that the collector is attempting to collect a debt and that any information obtained will be used for that purpose.\footnote{15 U.S.C. § 1692e(11) (2000).} The court found that although AT&T did fit the definition of a debt collector under the Act, the plaintiffs were not the consumers the law seeks to protect, since they were not the persons obligated to pay the debt being collected – their daughter-in-law was.\footnote{Conboy, 84 F. Supp. 2d at 504.} Therefore, plaintiffs could not state a claim under this section.

The court in \textit{Warner v. American Cablevision of Kansas City Inc.}\footnote{Id. at § 551.} held that all violations of the disclosure and record keeping provisions of the Cable Communications Policy Act\footnote{47 U.S.C. § 521 (2000).} are actionable. The plaintiff, a former customer of the defendant, brought suit under section 551 of the Act, which requires cable operators to disclose to customers the personal information that the operator retains, the purposes for which the information is retained, the circumstances under which the information will be disclosed to third parties, and the time after which the information will be destroyed.\footnote{Id. at § 551.}
In *Warner*, the plaintiff claimed that the defendant cable company failed to provide him with any Section 551 disclosure when the parties entered into a contract for cable service and that the notice plaintiff eventually did receive was so vague as to be violative of the Act's provisions.\(^{153}\) The court agreed, finding that American violated the Act by failing to provide Warner with the disclosure statement at the time of installation, and by failing to specify the type of customer information retained, for what purposes the information would be retained, to whom the information might be disclosed, and for how long the information would be retained.\(^{154}\)

The defendant argued that, despite the fact that it did indeed violate the disclosure requirement, Warner was not entitled to damages because he had not suffered actual injury.\(^{155}\) The court disagreed and held that no showing of actual damages was required for an aggrieved party to recover under the Act.\(^{156}\) The court based its reasoning on the Act itself, which states that "any person aggrieved" by a cable operator's violation of Section 551 may bring a civil action and may recover a maximum of $1,000 per violation.\(^{157}\) The court ultimately concluded that the plaintiff was aggrieved by two violations by the defendant, and awarded $2,000 in damages and attorneys fees.\(^{158}\)

Since no federal statute exists specifically regulating the collection and dissemination of personal information (at least that of consumers over the age of 13) via the Internet, some parties resorted to litigating under federal unfair trade practice law, state consumer protection and false advertising laws, and common law claims of invasion of privacy and trespass to chattels.

In February 2000, in anticipation that DoubleClick Inc. would merge its online profiles with the personally identifiable information in Abacus-Direct’s customer database, the Electronic Privacy Information Center (EPIC) filed a complaint against

---


\(^{154}\) Id. at 856-857.

\(^{155}\) Id. at 858.

\(^{156}\) Id.


DoubleClick with the Federal Trade Commission.\textsuperscript{159} EPIC stated that its interests in the matter were the protection of individual privacy and the danger that misuse of personal information posed to opportunities for individuals to secure employment, insurance, credit, medical services, and due process of law.\textsuperscript{160} EPIC also outlined DoubleClick’s frequent and sometimes drastic changes in its privacy policy, which originally assured users that the company had no knowledge of personally identifiable information of anyone who visited a Web site in the company’s network. The policy was later altered to allow for collection of information identifying an individual user’s server and browser type, which would be shared with third party advertisers.\textsuperscript{161} Upon completion of its merger with Abacus Direct, DoubleClick announced that it would begin associating names and addresses of users with its online profiles through the use of a match code contained in its cookies. Members of the newly formed Abacus Alliance (formerly the DoubleClick Network) would post provisions on their Web site giving users notice and choice as to the sharing of the compiled information.\textsuperscript{162} EPIC emphasized that the majority of Internet users who receive cookies from DoubleClick and already have their information in the Abacus database never visit the Web sites which detail the company’s collection practices and explain procedures for opting out of the information collection scheme.\textsuperscript{163} EPIC brought its claim under Section 5(a) of the FTC Act, which prohibits unfair or deceptive practices in or affecting commerce.\textsuperscript{164} Specifically, EPIC alleged that: (1) DoubleClick publicly represented that any user information it collected was and would remain anonymous; and (2) DoubleClick intended to combine its “anonymous” user information with users’ names, addresses, and purchase histories in its Abacus database.\textsuperscript{165} The complaint further alleged that DoubleClick’s conduct was likely to cause substantial

\begin{itemize}
\item \textsuperscript{159} See supra note 4.
\item \textsuperscript{160} Id. at 2.
\item \textsuperscript{161} Id. at 4, 5.
\item \textsuperscript{162} Id. at 7.
\item \textsuperscript{163} Id. at 8.
\item \textsuperscript{164} 15 U.S.C. § 45(a) (2000).
\item \textsuperscript{165} See supra note 4 at 9, 10.
\end{itemize}
injury to consumers, i.e. invasion of privacy, that was not reasonably avoidable by consumers and was not outweighed by countervailing benefits to consumers or competition.\textsuperscript{166} EPIC requested relief in the following forms: (1) an investigation into DoubleClick’s information collection and advertising practices; (2) the destruction of user records created when DoubleClick and its partners assured anonymity of such information; (3) an order to DoubleClick to obtain express consent from any user about whom it intended to create a personally-identifiable record; (4) civil penalties in an amount equal to 50\% of the revenues DoubleClick obtained as a result of the practices alleged in the complaint; (5) a permanent injunction against DoubleClick violating the FTC Act; and (6) compensatory damages to redress injury to consumers as a result of DoubleClick’s violations.\textsuperscript{167}

In the same week, Michigan Attorney General Jennifer Granholm filed a notice of intended action to file a lawsuit under the Michigan Consumer Protection Act.\textsuperscript{168} Granholm alleged the same facts EPIC did as to DoubleClick’s conduct concerning its data collection practices and its combination with Abacus Direct, emphasizing the company’s repeated changes of its privacy policy as a “moving target.”\textsuperscript{169} Granholm claimed that DoubleClick’s opt-out method did not provide consumers with adequate notice and choice as to the collection and use of personal information, that the placement of cookies on users’ computers was unknown and unauthorized, that DoubleClick’s promise that user information would remain anonymous was false and misleading, and that DoubleClick failed to disclose the intended use of the information it collected and to obtain knowing consent from consumers before gathering information.\textsuperscript{170} Each of these behaviors constituted a violation of the Michigan Consumer Protection Act.\textsuperscript{171} Granholm’s complaint also alleged common

\textsuperscript{166} Id. at 10
\textsuperscript{167} Id. at 11.
\textsuperscript{168} MSA § 19.418(1).
\textsuperscript{170} Id. at 8.
\textsuperscript{171} Id.
law claims of invasion of consumer privacy, conversion of consumers’ property rights in the value of their personal information, trespass to chattels (i.e. DoubleClick’s placement of cookies on users’ hard drives without their knowledge or consent), and promissory estoppel in that consumers detrimentally relied on DoubleClick’s promises of user anonymity. If DoubleClick did not submit an assurance of discontinuance, Granholm stated she would file suit seeking injunctive relief, civil penalties of up to $25,000 for each violation of the Michigan Consumer Protection Act, as well as a class action on behalf of Michigan consumers injured by DoubleClick’s conduct.

Around the same time as the previous actions were filed, Harriett Judnick brought another suit against DoubleClick and 200 of its network affiliates in California state court. Again, Judnick alleged the same facts concerning DoubleClick’s collection and disclosure of Internet users’ personal information and sought relief under claims of invasion of privacy and false and misleading advertising. Judnick’s first count alleged that Internet users have a reasonable expectation of privacy when visiting Web sites and purchasing products online, and that DoubleClick and its affiliates failed to provide users with adequate notice as to their information collection practices, adequate means of preventing collection of personal information, adequate means of reclaiming information already collected, and adequate means of safeguarding against inadvertent disclosure of information to unaffiliated third parties. Such conduct, plaintiff claimed, violated users’ right to privacy guaranteed under Article I, Section 1 of the California Constitution and constituted unlawful, misleading, fraudulent, and unfair business practices under the California Business and Professions Code. Judnick also alleged that DoubleClick and its affiliates were liable for false and misleading advertising in that

172 Id. at 8, 9
173 Id. at 13.
175 Id. at 5-8.
176 CAL. CONST. art. I, § 1.
they provided the public with assurances (via privacy policies) that no user information was being collected, retained, or disclosed, but required users to take affirmative steps to opt out of information collection despite reasonable expectations by users (based on defendants’ assurances) that no such practice was taking place.\footnote{\textit{See supra} note 174 at 9, 10.} In relief, the plaintiff sought to enjoin DoubleClick and its affiliates from using cookies and related technology to identify users without first obtaining consent; to require the defendants to provide users with an easy mechanism to destroy mistakenly gathered personal information and mistakenly created cookies or mistakenly created links between the two; to require DoubleClick to destroy all records personally identifiable user information obtained without consent; and to require DoubleClick and its affiliates to declare publicly and prominently that the company had obtained personally identifiable user information without consent and that henceforth that information would not be acquired without express user consent.\footnote{Id. at 10, 11.}


In March 2001, the United States District Court for the Southern District of New York dismissed a class action suit against DoubleClick, holding that the plaintiffs in that case had failed to state a viable claim.\footnote{In Re DoubleClick, Inc. Privacy Litigation, Case No. 00 Civ 0641 (NRB) (S.D.N.Y. 2001). See Michael A. Riccardi, \textit{DoubleClick Can Keep Hand in Cookie Jar, Federal Judge Rules}, NEW YORK LAW JOURNAL, March 30, 2001 (visited March 30, 2001) <http://biz.yahoo.com/law/010330/62999-6.html>.} Specifically, the court found that the
plaintiffs failed to allege that DoubleClick gained unauthorized access to their personal computers through its transmission of cookies.\footnote{183 Id.} DoubleClick obtained legitimate access to users' computers through the affiliated web sites within its advertising network, the court stated.\footnote{184 Id.} Plaintiffs' submissions to these affiliated web sites were intended and directed to those sites, whose authorization was sufficient to justify DoubleClick's access thereto, the court further held.\footnote{185 Id.} Finally, the court ruled that the information gathered by DoubleClick was similar to that collected on all consumers and that the value of such information represented no damage to consumers or unjust enrichment to collectors.\footnote{186 Id.}

### III. PROPOSED FEDERAL LEGISLATION

The Consumer Privacy Protection Act of 2000 (S. 2606) was introduced the day after FTC issued its report to Congress\footnote{187 See supra note 70.} and for the purpose of preemiting inconsistent state laws, establishing a strong federal standard for online privacy, and ensuring business certainty in the marketplace.\footnote{188 146 CONG. REC. S4299 (daily ed. May 23, 2000) (statement of Sen. Hollings).} The bill incorporates the code of fair information practices, established by the Health, Education, and Welfare Advisory Committee on Automated Data Systems in a 1973.\footnote{189 Id. See also EPIC, The Code of Fair Information Practices (visited Nov. 11, 2000) <www.epic.org/privacy/consumer/code_fair_info.html>.} These practices stress: 1) notice to and 2) consent by the person whose information is being collected, 3) access to that information by the person from whom it is collected, and 4) security of collected information.\footnote{190 146 CONG. REC. S4299.} The bill's sponsor, Senator Hollings, argued at its introduction that most Americans are
unaware of the threat the Internet can pose to consumer privacy, and that others’ fear of the loss of their privacy “represents the last hurdle impeding their full embrace of this exciting and promising new medium.”

The bill advocates an opt-in approach to the collection of data, as opposed to the opt-out approach currently in use and of which many consumers are not aware. The bill would also require Internet companies to notify consumers of changes to their privacy and information policies and not to use information gathered under outdated policies. Furthermore, the act would compel companies to keep consumers’ privacy preferences permanent, would provide protection for whistleblowers whose companies violate their privacy policies, would empower state attorneys general to enforce the act’s provisions on behalf of their constituents, would provide a private right of action for consumers harmed by the practices of data collectors, and would declare personal information not to be an asset in the case of a company collecting it declaring bankruptcy.

S. 2606 mandates that Internet users, when asked to divulge personal information have: clear and conspicuous notice that personal information is being collected; clear and conspicuous notice as to the gatherer’s intent in collecting the information; the ability to control the extent to which personal information about them is collected; and the right to prohibit unauthorized use, reuse, disclosure, transfer, or sale of the information collected.

Title I of the bill prohibits Internet service providers (ISPs) and commercial web site operators from collecting personally identifiable user information without giving users clear and conspicuous notice to users in a manner reasonable calculated to provide actual notice to users that information is being collected. Said notice must disclose: (1) what information will be collected; (2) the methods employed in collecting and using personal

---

191 Id.
192 Id. at S4300.
193 Id. at S4301.
194 Id.
195 S. 2606, Findings, § 2 (16).
information; and (3) all disclosure practices of the ISP or site operator regarding the collected information, including disclosure to third parties.\(^\text{196}\) The bill further prohibits ISPs and web operators from collecting information without users’ affirmative consent in advance.\(^\text{197}\) S. 2606 orders ISPs and operators to provide users reasonable access to their collected information upon request as well as reasonable opportunity for users to correct, delete, and supplement any information collected.\(^\text{198}\)

Under the act, ISPs and web operators commit breaches of privacy if they collect, disclose, or use personal information without providing notice to or obtaining consent from the user and if they know that the security, confidentiality, and integrity of user personal information is compromised by an act or failure to act on the part of ISPs or operators.\(^\text{199}\) A provision of S. 2606 makes the act applicable to third parties that use ISPs or commercial web sites to collect information about users of the services or web sites.\(^\text{200}\) An entity like DoubleClick would constitute such a third party.

The Act does limit liability for potential privacy breaches by allowing ISPs and web operators to collect, disclose, and use personal information “in order to protect the security and integrity of the service or web site” or in order “to conduct a transaction or to complete an arrangement for which a user has provided information.” Furthermore, ISPs and operators would not be liable for disclosures made in good faith and following reasonable procedures in responding to requests for disclosures of information under COPPA to parents of children whose information has been collected.\(^\text{201}\) An exception also applies for disclosure of personal information in response to warrants or court orders granted on a showing of compelling need for the information.\(^\text{202}\)

\(^{196}\) Id. at § 102 (a) (1) – (3).
\(^{197}\) Id. at § 102 (b).
\(^{198}\) Id. at § 102 (c).
\(^{199}\) Id. at § 102 (f) (1), (2).
\(^{200}\) Id. at § 102 (g).
\(^{201}\) Id. at § 104 (a), (b).
\(^{202}\) Id. at § 106.
A breach of user privacy under the S. 2606 would be treated as an unfair or deceptive trade practice for purposes of litigation and enforcement by the FTC.\textsuperscript{203} Individuals harmed under the act would have a private right of action to sue in state court to enjoin violations and/or recover their actual monetary loss or $5,000 for each violation, whichever is greater.\textsuperscript{204} Courts would be allowed to award up to $50,000 for willful and knowing violations of the act as well as punitive damages and attorneys fees.\textsuperscript{205}

Perhaps the most drastic measure contained in the bill is the order to the FTC to establish the Office of Online Privacy to study and monitor privacy issues concerning e-commerce and the Internet as well as the operation and effectiveness of the act itself.\textsuperscript{206} This agency would report its findings and recommendations to the FTC and the House and Senate Commerce Committees.

Similar bills were proposed in the 106\textsuperscript{th} Congress by Senators McCain and Toricelli. Senator McCain's bill, the Consumer Internet Privacy Enhancement Act (S. 2928) would require web operators to give notice of their information practices to users as well as provide obvious opt-out mechanisms.\textsuperscript{207} The bill would also prevent the collection of personal information unless users are given the opportunity to opt-out of disclosure of the information and for use beyond the primary purpose for which it has been collected. The Secure Online Communication Enforcement Act (S. 2063), sponsored by Senator Toricelli, would amend Title 18 of

\textsuperscript{203} Id. at §§ 301, 302.
\textsuperscript{204} Id. at § 303.
\textsuperscript{205} Id.
\textsuperscript{206} Id. at § 307.
\textsuperscript{207} S. 2928, 106th Cong. (2000). The bill would forbid commercial web site operators to collect personal information from users unless: (1) operators provide detailed notice that information is being collected and for what purpose, and (2) opportunities for users to limit use of the collected information for marketing purposes. The bill provides a safe harbor for operators who comply with self-regulatory guidelines issued by industry seal programs or approved by the FTC. Noticeably absent from the text of the bill are liability for Internet service providers and private rights of action for violations.
the United States Code to extend restrictions on disclosure of personal information to web site operators.\textsuperscript{208}

\section*{IV. ANALYSIS}

Given at least one court’s hostility to government regulation mandating an opt-in approach to collection and sharing of consumers’ personal information and patterns of communication,\textsuperscript{209} legislation like Senator Hollings’ bill may face harsh constitutional tests. However, courts tend to grant more deference to measures specifically mandated by Congress than to those promulgated by regulatory agencies. Such deference was granted to the privacy measures contained in the Cable Communications Policy Act\textsuperscript{210} as well as to similar provisions in the Telecommunications Act (just not to the particular rules generated by the FCC under the Act).\textsuperscript{211}

\subsection*{A. Central Hudson Test}

In determining whether a restriction on the collection and dispersal of consumer information would be constitutional, courts would most likely construe the measure as a potential restriction on commercial speech and apply a \textit{Central Hudson} test,\textsuperscript{212} as did the Tenth Circuit in \textit{U.S. West}. The test allows regulation on commercial speech, provided it is neither misleading nor

\begin{itemize}
\item \textsuperscript{208} S. 2063, 106th Cong. (2000). The bill would allow ISPs and web operators to disclose personal user information to third parties only if the disclosure is: (1) necessary to initiate, provide, and collect for access and/or services rendered; (2) necessary to protect the rights or property of the provider; (3) requested by the user; (4) made with the consent of the user at the time disclosure is sought; or (5) required by law. The bill would place no restrictions on ISPs’ and operators’ use or disclosure of aggregate user information (i.e. anonymous on-line profiles).
\item \textsuperscript{209} \textit{See U.S. West}, 182 F.3d 1224 (10th Cir. 1999).
\item \textsuperscript{211} \textit{U.S. West}, 182 F.3d 1224 (10th Cir. 1999).
\item \textsuperscript{212} \textit{Central Hudson}, 447 U.S. 557 (1980).
\end{itemize}
advocating illegal activity, if: (1) there is a substantial government interest at stake; (2) the regulation directly advances that government interest; and (3) the regulation is narrowly tailored and not overly restrictive in fulfilling the government interest. Additionally, the restriction need not be the least restrictive one conceivable, but merely reasonable in proportion to the interest served.

In the case of the Consumer Privacy Protection Act, the most apparent government interest at stake is personal privacy, a right established and reinforced in decisions such as *Griswold v. Connecticut* and *Roe v. Wade*. The bill’s other stated purposes are those of establishing a uniform standard for online privacy and ensuring business certainty in the marketplace, both obvious legitimate government interests. The Act directly advances these interests in that it ensures consequences and remedies for unlawful breaches of consumer privacy and by establishing minimum uniform standards by which web operators must abide with regard to collection and use of personal information. Satisfying the third prong of the *Central Hudson* test could prove problematic, especially if courts follow the Tenth Circuit’s precedent in *U.S. West*. In that case, the majority favored an opt-out approach to the collection and sharing of consumer information, as opposed to the opt-in approach espoused by the Consumer Privacy Protection Act. The Tenth Circuit found that the opt-in approach adopted by the FCC was not narrowly tailored and impinging on communications providers’ right to free and unfettered commercial speech, and thus failed the *Central Hudson* test’s third prong. However, the dissent in *U.S. West* argued that the opt-out approach failed to fulfill the Congressional goal (as stated in the Telecommunications Act) of informed consumer

---

213 Id.
214 Board of Trustees of State Univ. of N.Y. v. Fox, 492 U.S. 469, 480 (1989).
215 381 U.S. 479 (1965).
217 See supra note 188.
consent to the collection and sharing of personal information.\footnote{Id. at 1247.}
Provided courts take notice of the Act's express goal of informed consumer consent and grant it the status of legitimate government interest, the opt-in method would likely be deemed to advance directly consumer privacy and to do so in a reasonably narrowly tailored manner.

**B. Improvements over prior legislation**

As made evident by the cases mentioned earlier this article, current laws dealing with the collection, dispersal, and retention of consumer personal information rarely provide consumers with a private right of action, and in the rare case that a law does, it usually only provides such a right to a very narrow class of potential litigants.

Under *U.S. West*, courts appear loath to enforce regulatory measures not specifically required by Congress (i.e., the FCC's opt-in approach to collection and sharing of telephone customers' personal data).\footnote{Id.} Courts also seem reluctant to allow suits under laws which provide no private right of action for claims involving disclosure of consumer information to third parties. In *Conboy*, even though the court found that defendant may well have violated an FCC regulation prohibiting disclosure of telephone customer information to third parties, it determined that no private right of action existed and thus barred the plaintiffs' claim.\footnote{Conboy, 84 F. Supp. 2d 492, at 500-502.} In *Warner*, the court allowed recovery only because a private right of action was explicitly stated in the Cable Communications Policy Act.\footnote{Warner, 699 F. Supp. 851, at 858.} Furthermore, as was illustrated by the recent decision of the Southern District of New York,\footnote{In Re DoubleClick, Case No. 00 Civ 0641.} courts will not allow recovery when plaintiffs are not able to prove any damages. Seemingly, damages may be presumed when a statute provides a private right
of action, as the court did in applying the law at issue in Warner.\textsuperscript{224} Finally, courts seem to be wary of involving third parties in the relationships between consumers and primary service providers, in which statutory obligations as to non-disclosure usually arise. This was the case in Conboy, in which the court stated that a long distance provider was not under the same obligation of non-disclosure as the local telephone service provider.\textsuperscript{225} The same approach was taken by the court in the class action suit against DoubleClick, in which the court held that authorized access by one party to a user’s personal computer allowed access by additional parties.\textsuperscript{226}

The Consumer Privacy Protection Act could conceivably close these apparent judicial loopholes for web operators. First, the act specifically orders an opt-in approach to be employed in web operators’ information practices,\textsuperscript{227} leaving no question as to the preferred Congressional method of achieving the act’s stated goal and advancing its stated interest. Second, the court explicitly grants consumers whose information is collected and shared in violation of the act a private right of action, leaving no dispute as to whether one exists or whether plaintiffs must prove damage under tort or unfair trade practice theories.\textsuperscript{228} Finally, the act states that its provisions are applicable to third parties that use ISPs or web sites to gather information regarding other users, solidifying such parties’ liability as to the collection and use of personal consumer information.\textsuperscript{229}

\textbf{C. Problems with similar legislative proposals}

The Consumer Internet Privacy Enhancement Act (S. 2928) would certainly be an improvement over prior existing and nonexisting federal and state laws. Of the Internet privacy bills to

\begin{footnotes}
\item[224] 699 F. Supp. 851, at 858.
\item[225] Conboy, 84 F. Supp 2d 492, at 499.
\item[226] In Re DoubleClick, Case No. 00 Civ. 0641.
\item[227] S. 2606, Findings, § 2 (16).
\item[228] Id. at § 303.
\item[229] Id. at § 102 (g).
\end{footnotes}
come out of the 106th Congress, it provides the most comprehensive and detailed and detailed requirements with regards to notice to consumers of web operators’ information collection and use practices. However, some experts have argued that the amount of information required in such notices could overwhelm Internet users, who tend to favor speed and convenience when searching for information on commercial web sites. The act’s emphasis on the notice provision of Fair Information Practices comes at a cost to the principles of consent and access, neither of which are explicitly given effect by the bill. Furthermore, while S. 2928 does provide a number of civil penalties for violations of its provisions, visibly absent from its language is a private right of action by which consumers themselves may enforce their right to privacy. Finally, the bill provides a safe harbor for operators who comply with self-regulatory guidelines issued by industry group privacy seal programs or the act’s notice requirements. Such an allowance, especially in the absence of a private right of action, could leave enforcement of privacy standards up to web operators themselves, a practice whose effectiveness has proven unsatisfactory to the public and to the FTC.

---

230 S. 2928 § 2 (b) (1) (A) – (H). The Act would require operators to disclose: their identities as well as those of third parties whom the operator knowingly permits to collect information through their sites; the types of information likely to be collected; descriptions of how operators plan to use such information, including availability to third parties; the categories of potential recipients of information submitted; whether users must surrender personal information in order to use web sites; descriptions of what steps operators take to secure collected personal information; descriptions of means by which users may elect not to have their information made available to third parties; and contact information for web operators.


232 Id.

233 S. 2928 § 2 (d) (1), (2).

234 See supra note 70.
The Secure Online Communication Enforcement Act (S. 2063) allows disclosure of personal information by web operators to non-government entities only if such disclosure is necessary to execute a transaction related to the use of a site or service, necessary to protect the rights or property of the operator, the disclosure is made at the request or with the consent of a customer, or is required by law.\textsuperscript{235} The act further provides that ISPs and web operators may not refuse service to or access to users who refuse to consent to the disclosure of their information.\textsuperscript{236} However, S. 2063 specifically allows ISPs, web operators, and third parties to use and disclose aggregate customer subscriber information from which personally identifiable characteristics have been removed.\textsuperscript{237} Such information, despite the fact that it may not be personally identifiable, could include records of web sites visited and transactions made by individual users, and would resemble, in essence, the online profiles complied by companies like DoubleClick, who use such information to target advertising and commercial solicitations to those individuals. Coupled with its lack of effort to incorporate all of the established Fair Information Practices, the provisions of S. 2063 appear inadequate to meet the privacy needs and expectations of current and potential Internet users.

V. CONCLUSION

Although some Internet users may deem targeted web advertising and commercial emails innocuous and merely inconvenient, many relish the anonymity that the Internet can and, many feel, should allow and maintain. Given that individual privacy has been well established as a right in American constitutional law, consumers should not need to resort to self-help and the aid of third parties in guaranteeing their privacy. Privacy-minded Internet users believe they should not have to seek out and

\textsuperscript{235} S. 2063 § 3 (b) (i)-(v).
\textsuperscript{236} Id. at § 3 (e).
\textsuperscript{237} Id. at § 3 (d).
wade through pages of preferences in order to make clear to ISPs and web operators exactly what information should and should not be made available for all the world to see. Furthermore, advocates believe that privacy should not come at the price paid for downloadable software and other external measures, around which backdoors are bound to be discovered sooner or later. Such beliefs have been made evident by the rash of lawsuits filed by Internet users in the past year, seeking to impose penalties on operators who collect and share information without notice or consent. These lawsuits have also made evident the need for a statutory private right of action, since plaintiffs are rarely provided adequate relief, if any at all, from the buying and selling of their identities and their personal surfing habits.

Industry self-regulation has also failed to provide many users with their desired minimum levels of privacy protection. Reports and sanctions of seal program violations are few and far between, and rarely result in any repercussions for the perpetrators. Further, the standards for self-regulation can and do vary, and their effectiveness can fluctuate according to the price paid for certification. Individual state laws are equally likely to vary as to minimum standards, and the fluid nature of Internet communications is likely to cause problems as to determinations of jurisdiction and the overall effectiveness of state enforcement. The passage of a comprehensive federal law that incorporates widely recognized privacy principles, establishes minimum privacy standards, provides individuals with a private right of action for breaches of privacy, and closes potential loopholes would be a substantial step toward the solution of this problem. The Consumer Privacy Protection Act does just that.

Ethan Hayward