3 SITE BUYERS
03.

Mid 620698-000

herly Millenium Direct Inc.), 318 In-
FL 33326. Phone 561-362-6722.

ON
credit cards to receive live video-
2.

UNTS
Counts Thru: Feb 2002

	Total Number	Price per/M
	1,817,960	80.00
	102,260	85.00
	102,260	*250.00

tra; key coding, 1.00/M extra.
POLICY
rs. 15% commission to agencies.
r mail date. Cancel charges: Or-
original mail date will be billed a
payment required for new custom-
NG
.00/M extra; mag tape, 30.00 fee.

OM POSTAL ADDRESS FILE
002.

Mid 736743-000

il, Inc., 1250 Broadway, New York,
1-7100. Fax 212-760-1774.
edia.com
ealmedia.com
Manager—Amy Gosman, Phone
7media.com
ON
it Scholarships.com to explore the
aid opportunities they could be eli-
gistration internet.
UNTS
Counts Thru: Jun 2002

	Total Number	Price per/M
	1,503,447	*80.00
	50,000	+15.00
	372,173	75.00
	704,724	"
	78,813	"
tudents	110,992	"
	121,242	"

; gender, state, SCF, Zip, 5.00/M
5.00/M extra; telephone numbers,
obbies, hotline (60 day), academic/
a of study/intended major, school
D scores, class standing, current
involved with, college attending,
athletic ability, religion, hobbies,
POLICY
rs. Payment due 30 days after mail
cancelled orders will be billed at a
cancelled after mail date require

RST TIME COMPUTER POSTAL ADDRESSES
002.

Mid 721843-000

n List Counsel, Inc., 4300 US High-
ton, NJ 08543. Toll Free 800-252-
Phone 609-580-2765.
t.com
ON
net devices at their postal address.
gistration.
UNTS
Counts Thru: Jan 2001

	Total Number	Price per/M
	991,231	105.00
	325,957	+6.00
	540,921	"
	891,466	+11.00
	99,765	"
	132,523	+16.00
	272,884	+11.00
	629,182	+6.00
ory:		
	27,425	+11.00
	24,943	"
	33,990	"
	37,133	"
	45,396	"
	42,917	"
	19,705	"
	47,631	"
	29,420	"
	39,501	"
	57,238	"
	27,543	"
	29,459	"
	37,852	"
	36,814	"
	26,245	"
	48,164	"
	53,673	"

EMAIL & POSTAL LISTS FROM MARKETSONDEMAND

Data Verified: Nov 15, 2002.

ocation ID: 10 DCLS 552 — Mid 740127-00(

MarketsOnDemand, 57 W. Grand Ave., 2nd Fl., Chicago, IL 60610. Phone 866-494-1432.
URL: http://www.marketsondemand.net

. PERSONNEL
Sales Department
E-mail: sales@marketsondemand.net

. SUMMARY DESCRIPTION
Source of fresh consumer data generated entirely online including e-mail and postal addresses.

. LIST SOURCE
Internet/online/website registration Online.

. SELECTIONS WITH COUNTS
Updated: Jun 27, 2002.

	Total Number	Price per/M
Email address	9,500,000	*75.0(
Postal address	14,500,000	"
Both	9,500,000	150.0(
Gender:		
Male	2,839,000	+2.5(
Female	2,915,000	"
Marital status:		
Single		
Married		
Seperated/divorced		
Widowed		
Domestic partner		
Age:		
18-24		
25-34		
35-44		
45-54		
55-64		
65 and over		
Registered web site member		
Computer site		
ISP site		
Job site		
Music site		
Online gaming site	1,875,000	"
Shopping site	403,000	"
Student scholarship site	293,000	"
Sweepstake entrants	1,115,000	"
Income:		
Under 15,000	656,000	+7.50
15,000-29,999	1,216,000	"
30,000-49,999	1,286,000	"
50,000-74,999	993,000	"
75,000-99,999	391,000	"
100,000-149,999	278,000	"
150,000+	161,000	"
Interests:		
Antiques	79,000	+10.00
Arts & entertainment	366,000	"
Auctions	83,000	"
Automotive	73,000	"
Beauty & cosmetics	93,000	"
Books & magazines	366,000	"
Business	220,000	"
Casino games & lotteries	122,000	"
Cell phones & pagers	18,000	"
Children's merchandise	170,000	"
Collectibles	90,000	"
Cooking, food & wine	272,000	"
Crafts & hobbies	245,000	"
Electronics	244,000	"
Family/parenting	162,000	"
Fashion & apparel	167,000	"
Free stuff	369,000	"
Games, contests & sweeps	251,000	"
Gardening	123,000	"
Gifts	110,000	"
Health & fitness	605,000	"
Home decorating	117,000	"
Home improvement	190,000	"
Internet (surfing, chat)	33,000	"
Internet technology	75,000	"
Investing & finance (general)	656,000	"
Annuities	3,000	"
Bonds	6,000	"
CDs/Money market funds	10,000	"
IRAs/401ks/Keoughs	17,000	"
Mutual funds	16,000	"
Real estate/land	18,000	"
Stocks	60,000	"
Music (general)	656,000	"
Alternative	18,000	"
Christian	16,000	"
Classic opera	10,000	"
Country western	31,000	"
Heavy metal	12,000	"
Jazz/new age	14,000	"
Oldies	38,000	"
Rhythm & blues	55,000	"
Pop & rock	53,000	"
Outdoor enthusiasts	115,000	"
PCs (general)	958,000	"
Hand-held devices	17,000	"
Hardware	38,000	"
Networking	41,000	"
Peripherals	73,000	"
Software	200,000	"
Pets (general)	186,000	"
Cats	3,000	"
Dogs		
Self-improvement		
Sewing		
Shopping (general)		
Catalog		
Online		
Retail		
Sports (general)		
Auto racing		
Baseball		
Basketball		
Football		
Golf		
Skiing		
Tennis	12,000	"
Surveys	111,000	"
Travel	194,000	"
Business	33,000	"
Vacation	21,000	"

(*) 10% discount for qualified non-profit fundraising organizations (on base rate only); one time reuse, 50% off base rate.
Minimum order 5,000.

A. OTHER SELECTIONS
State, SCF; address type, 1.50/M extra; city & state, DMA code, DMA county size, Metropolitan Statistical Area (MSA), Zip, 2.50/M extra; area code, 3.00/M extra; demographic se-

1-800-FLOWERS INTERNET BUYERS

Data Verified: Dec 26, 2002.

Location ID: 10 DCLS 554 — Mid 671636-000

1. PERSONNEL
List Manager — Millard Group, Inc., 10 Vose Farm Rd., Peterborough, NH 03458. Phone 603-924-9262. Fax 603-924-9420.
URL: http://www.millard.com

2. SUMMARY DESCRIPTION
Internet buyers of floral arrangements, plants and gifts.
55% male, 45% female; average age 35.

3. LIST SOURCE
Internet/online/website registration internet.

4. SELECTIONS WITH COUNTS
Updated: Dec 26, 2002 — Counts Thru: Nov 2002

	Total Number	Price per/M
Web buyers at postal address (1 month)	144,611	*147.00
3 month	419,188	*142.00
6 month	715,213	*137.00
12 month	1,596,972	*125.00

(*) Selection charges included in rates.
Competitive rate, 20.00/M.
Net name arrangement (50,000 minimum), 85% plus 8.00/M run charge.

Privacy Self Regulation:
A Decade of Disappointment
Chris Jay Hoofnagle
March 4, 2005

Sample mailing piece required.

11. MAINTENANCE
Updated monthly.

DIRECTQLICK.COM - POSTAL

Data Verified: Oct 15, 2002.

Location ID: 10 DCLS 552 — Mid 766506-000

1. PERSONNEL
List Manager — ClientLogic Specialists Marketing Services, 1200 Harbor Blvd., 9th Fl., Weehawken, NJ 07087. Phone 201-865-5800. Fax 201-867-2450.
URL: http://www.clientlogic.com
E-mail: listinfo@clientlogic.com
Key Contact: Karen Isenberg
E-mail: karenise@clientlogic.com

2. SUMMARY DESCRIPTION
Members who have received on offer via email, opened the email and responded by clicking on the link provided.
46% male, 48% female; ages 26-39.

3. LIST SOURCE
Internet/online/website registration, direct response.

4. SELECTIONS WITH COUNTS
Updated: Oct 15, 2002.

	Total Number	Price per/M
Total file	11,486,453	75.00
Hotline (monthly)	390,000	85.00

Minimum order 5,000.

4A. OTHER SELECTIONS
Geographic, gender, 6.00/M extra; age, 11.00/M extra; Canadian, interest, homeowner, category, 16.00/M extra; responder, 26.00/M extra.

5. COMMISSION, CREDIT POLICY
Cancel charges: Orders cancelled after mail date will be charged full rental. Orders received and processed will be subject to a 50.00 flat cancellation fee and running charges.

6. METHOD OF ADDRESSING
Diskette, 50.00 fee; e-mail, 30.00 fee; CD-Rom, 30.00 fee; cartridge, 30.00 fee; FTP, 50.00 fee.

8. RESTRICTIONS
Sample mailing piece required.

11. MAINTENANCE
Updated 12 times per year.

AUTO CREDIT FINDERS.COM

Data Verified: Jan 23, 2003.

Location ID: 10 DCLS 508 — Mid 675048-000

1. PERSONNEL
List Manager — TCI List Management Direct, Inc., 10911 Riverside Drive, Toluca Lake, CA 91602. Phone 818-752-1800. Fax 818-752-1808.
E-mail: fxdirectcomputer@aol.com

2. SUMMARY DESCRIPTION
Autocreditfinders.com is a website that helps individuals with less then perfect credit find a car loan; respondents are completing an online loan application.
65% male, 35% female; average age 48.

3. LIST SOURCE

AMERICAN INDEX - AILMENT SUFFERERS MASTERFILE

Data Verified: Nov 16, 2002.

Location ID: 10 DCLS 527 — Mid 764570-000

Compiled Solutions, 101 Morgan Lane, Suite 120, Plainsboro, NJ 08536. Phone 609-275-6452. Toll Free 800-585-5720. Fax 609-936-1918.
URL: http://www.compiledsolutions.net
E-mail: melbrecht@krolldirect.com

1. PERSONNEL
Acct Mgr

2. SUMMARY DESCRIPTION
Responders identified as one person suffering from one or more ailments, or multiple members of the household suffering from one or more ailments.

3. LIST SOURCE
Compiled, internet source survey respondents.

4. SELECTIONS WITH COUNTS
Updated: Sep 6, 2002.

	Total Number	Price per/M
Ailment sufferers	5,572,874	120.00
Multiple ailment sufferers	1,308,821	"
	419,390	+10.00
monthly)	137,000	+15.00
umbers	1,308,821	+25.00
ailment:		
ners	12,047	+10.00
	68,745	"
	205,155	"
	337,623	"
ain	502,825	"
/hair loss	242,599	"
problems	78,358	"
g gums/gum disease	110,635	"
pressure	324,650	"
sion	123,729	"
s	181,306	"
s-type 2	32,315	"
Eczema	116,026	"
Emphysema	31,136	"
Epilepsy	24,942	"
Estrogen	95,143	"
Gastritis	79,345	"
Frequent headaches	347,628	"
Frequent heartburn	245,827	"
Frequent migraines	323,010	"
Hearing problems/loss	155,601	"
Heart condition	103,877	"
High cholesterol	204,388	"
Impotence	8,931	"
Insomnia	195,203	"
Irritable bowel	20,635	"
Lactose intolerant	120,199	"
Multiple sclerosis	15,206	"
Obesity	48,575	"
Osteroporosis	48,368	"
Parkinson's disease	6,740	"
Physical handicap	60,908	"
Prostate	23,128	"
Rheumarthritis	27,163	"
Sensitive skin	299,649	"
Sinusitis problems	265,665	"
Spinal injury	5,250	"
Sports injury	135,673	"
Ulcer	80,164	"
Visual impairment	83,227	"
Wheel chair	2,750	"
Yeast infection	118,346	"
Demographic:		
Married	629,919	+10.00
Single	429,057	"
Divorced	151,718	"
Widowed	24,065	"
Cohabitating/living together	85,103	"
Income 15,000-19,999	108,711	"
Income 20,000-24,999	116,953	"
Income 25,000-29,999	110,725	"
Income 30,000-34,999	114,891	"
Income 35,000-39,999	92,928	"
Income 40,000-44,999	87,662	"
Income 45,000-49,999	75,568	"
Income 50,000-59,999	116,854	"
Income 60,000-74,999	131,321	"
Income 75,000-99,999	92,435	"
Income 100,000-124,999	45,505	"
Income 125,000+	39,502	"
Presence of child/children	153,276	"
High school graduate	377,104	"
Attended college	528,806	"
College graduate	170,056	"
Some post graduate studies	42,553	"
Masters degree	56,807	"
Doctorate degree	15,533	"
Business owner	28,917	"
Homemaker	76,543	"
Nurse	31,912	"
ional/technical	220,798	"
arketing	100,066	"
ry/clerical	134,675	"
abor	67,306	"
	141,971	"
	68,032	"
r	41,964	"
nanagement	51,868	"
	15,068	"
wner	630,825	"
artment	12,519	"
me	206,546	"
artment	235,656	"

Net name arrangement (minimum 50,000), 85% plus 10.00/M running charge.
Minimum order 5,000.

4A. OTHER SELECTIONS
State, SCF, SCF, 6.00/M extra; gender, demographics, 10.00/M extra; ailments, 15.00/M extra.

5. COMMISSION, CREDIT POLICY
Cancel charges: 50.00 flat cancellation fee on orders cancelled prior to mail date. Full charges apply on orders cancelled after mail date. 25% commission on base rate and selections.

20% commission to brokers. Payment due 30 days after mail date. Cancel charges: Orders cancelled after receiving date incur a 50.00 flat cancellation charge plus all select surcharges. Cancellations after mail date must be paid in full.

6. METHOD OF ADDRESSING
Cheshire labels, 4-up; pressure sensitive labels, 10.00/M extra; mag tape, 9T 1600 BPI, 25.00 fee; diskette, 25.00 fee; e-mail, 50.00 fee.

7. DELIVERY SCHEDULE
10 working days.

8. RESTRICTIONS
Two sample mailing pieces required.

LOCATE™ PLUS.com

May 21, 2004

Dear Consumer,

To answer your question of what rights you have over the information that we have about you, there are none. We are a third party data collection company and we import information about each subject from several different sources including credit bureaus and utility companies. If you find that the information supplied to you from us is inaccurate, you may take that up with those companies.

Thank you for using LocatePlus.

Anne Ouellette
LocatePlus.com Customer Service

LocatePlus.com, Inc.
64 Central Street
Georgetown, MA 01833
978.352.6633
fax: 978.352.7799
www.locateplus.com

Front and Back Covers: Personal information available for sale, priced per thousand names.
Inside Front Cover: Letter from Locateplus.com to concerned consumer forwarded to EPIC.
Inside Back Cover: Lists sold of Magazine Subscribers.

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Privacy Self Regulation: A Decade of Disappointment

Summary

The Federal Trade Commission (FTC) is capable of creating reasonable and effective privacy protections for American consumers. There is no better example of this than the Telemarketing Do-Not-Call Registry. The Registry, which was created and is now run by the FTC, makes it easy for individuals to opt-out of unwanted telemarketing. Now, more than 80 million numbers now no longer ring at the dinner hour.

Prior to the creation of the Registry, the telemarketing industry created self-regulatory protections that were largely useless. One had to write a letter to opt out of telemarketing, or pay to opt out by giving their credit card number to the Direct Marketing Association (DMA). The industry's self-regulatory efforts didn't even cover all telemarketers—only those that were members of the DMA. At its peak, the self-regulatory opt-out system had less then 5 million enrollments.

FTC's success in the telemarketing field demonstrates that it can protect Americans' privacy effectively and fairly. However, telemarketing was a 20th century problem. This report argues that it is time for the agency to move into the 21st century. It is time for the agency to apply the principles of telemarketing privacy regulation into the online world.

The FTC can protect privacy better than the industry can with self-regulation. We now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections.

New tracking technologies exist that individuals are unaware of, and old tracking technologies continue to be employed. Some companies deliberately obfuscate their practices so that consumers remain in the dark. Spyware has developed and flourished under self-regulation. Emerging technologies represent serious threats to privacy and are not addressed by self-regulation or law.

Self regulation has failed to produce easy to use anonymous payment mechanisms.

And finally, the worst identification and tracking policies from the online world are finding their way into the offline world. In other words, the lack of protection for privacy online not only has resulted in a more invasive web environment, but has also started to drag down the practices of ordinary, offline retailers.

EPIC calls upon the Federal Trade Commission and Congress to seriously reconsider its faith in self-regulatory privacy approaches. They have led to a decade of disappointment; one where Congress has been stalled and the public anesthetized, as privacy practices steadily worsened. We call on the government to create a floor of standards for protection of personal information based on Fair Information Practices.

I. The FTC Registry Is Better Than Market Alternatives

The Federal Trade Commission's (FTC) Telemarketing Do-Not-Call Registry was a stunning privacy success. Americans enrolled 10 million numbers in the Registry in its first day of operation. Now, the phone has stopped ringing on the more than 60 million numbers that were enrolled by the public. The nuisance of telemarketing will now be a thing of the past. Those who wish to receive telemarketing may still do so, but others have an easy option to preserve the dinner hour from interruption.

When one analyzes the decisions made by the FTC, it reveals that the agency took steps to effect consumers' desires. The FTC publicized the existence of the Registry and gave it a simple name and URL on the Internet. The FTC allowed people to enroll free by telephone or by the Internet. The FTC minimized "authentication" burdens. That is, the FTC made it easy for people to enroll by not requiring the consumer to jump through unnecessary hoops. Some from the industry suggested that only the line subscriber—not even a spouse or roommate—could enroll.

The Do-Not-Call Registry was a success because the FTC took the opposite approach from the self-regulatory system created by the Direct Marketing Association (DMA). In every respect, the FTC ensured that the Registry would be easy to use and fair, while the DMA's opt-out mechanism was difficult to use and relatively unknown.

For starters, the DMA's system only applied to the industry association's members. Telemarketers who had not joined the group were not bound to comply with consumers' desire to opt-out. The FTC's approach applied to a much broader group of telemarketers.

Second, the DMA's list was named the "Telephone Preference Service." The name and acronym, "TPS," had no meaning to the public. To some, it could mean a list of people who preferred to be telemarketed. The FTC approach, on the other hand, was sensibly named and assigned a easy to remember URL, http://donotcall.gov, on the Internet.

Third, the DMA's list required the consumer to actually write a letter for free enrollment. To enroll online, the consumer had to pay a fee and give their credit card number to the DMA. The FTC's approach allows free Internet, mail, and telephone enrollment.

The FTC's Registry is universal, free, and easy to use. Individuals could enroll online or by phone. The DMA's only applied to its members, cost money to enroll online, and was difficult to find. It's no wonder why the DMA's list only had 5 million enrollments, while the FTC's has more than 80 million.

These forces combined to make the DMA's market approach to telemarketing ineffective. The numbers speak for themselves. USA Today commented in 2002 that: "In 17 years, just 4.8 million consumers have signed up with the DMA's do-not-call list. By contrast, just five states -- New York, Kentucky, Indiana, Florida and Missouri -- have signed up roughly the same number in far less time."[i]

Today's self-regulatory approaches to Internet privacy are much like the failed ones employed by the DMA for telemarketing. They are difficult to use, confusing, and often offer no real protection at all. This report details the current state of privacy on the Internet, and illustrates the myriad ways in which threats to privacy are becoming ever more grave, as new

technologies are developed, new practices become commonplace, and companies are not held accountable for disregarding privacy risks. Collection of personal information on the Internet runs rampant, both through direct and indirect means, both in the open and in secret. It is imperative that the FTC act now to correct these market failures. The FTC effectively and fairly corrected the failures of a 20th century nuisance—telemarketing. It is time for the agency to move into the 21st century and correct the failures of self-regulation to meaningfully protect Internet privacy.

II. Ten Years of Self-Regulation and Still No Privacy In Sight

EPIC has completed three Surfer Beware reports assessing the state of privacy on the Internet. "Surfer Beware I: Personal Privacy and the Internet," a 1997 report, reviewed privacy practices of 100 of the most frequently visited web sites on the Internet. It checked for collection of personal information, establishment of privacy policies, cookie usage, and anonymous browsing. The inquiry found that few sites had easily accessible privacy policies, and none of these policies met basic standards for privacy protection. However, at that time, most of the sites surveyed allowed users to access web content and services without disclosing any personal data. The report ended with a recommendation of continuing support for anonymity and the development of both good privacy policies and practices.

In 1998, EPIC produced "Surfer Beware II: Notice Is Not Enough," a report based on a survey of the privacy practices of 76 new members of the Direct Marketing Association ("DMA"), a proponent of self-regulation of privacy protection. The DMA released guidelines in 1997 that would require all future members of the DMA to publicize privacy policies and provide an opt-out capability for information sharing. Of the 76 new members surveyed, only 40 had web sites, and only 8 of these sites had policies satisfying the DMA's requirements. The report concluded that DMA's self-regulation efforts were not effective.

Fair Information Practices

are commonly accepted responsibilities governing collection, access to, and control over personal information. They include:

- **Collection Limitation**: requires lawful, fair, and legitimate data collection.
- **Data Quality**: requires accuracy, completeness, and timeliness of data.
- **Purpose Specification**: requires entities to articulate why data is being requested and prohibits its use for other purposes.
- **Use Limitation**: requires consent for use of information inconsistent with the purpose of which it was collected.
- **Security Safeguards**: requires procedures to stop unauthorized access, use, modification, or disclosure of data.
- **Openness**: requires transparency of personal data practices, including notice of databases and the identity and location of the data controller.
- **Individual Participation**: requires access to, correction of, and sometimes destruction of personal information.
- **Accountability**: requires legal rights to ensure compliance.

The 1999 report "Surfer Beware III: Privacy Policies without Privacy Protection" assessed the privacy practices of the 100 most popular shopping web sites on the Internet. It examined whether these sites complied with common accepted privacy principles, used profile-based advertising, and employed cookies. The survey

determined that 18 of the sites had no privacy policy displayed, 35 of the sites used profile-based advertising, and 86 of the sites used cookies. None of the companies adequately addressed Fair Information Practices, commonly-accepted responsibilities covering collection, access to, and control over personal information. Surfer Beware III concluded that current practices of the online shopping industry provided little meaningful privacy protection for consumers.

The Federal Trade Commission ("FTC") has given self-regulation a decade to produce reasonable privacy protections online. The FTC first visited online privacy in 1995, and with minor fluctuations since then, has adopted a policy that embraces the idea that self-regulation is "the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology."[ii] It certainly is the least intrusive approach for companies exploiting personal information, but it has not efficiently ensured Fair Information Practices. Of the five Fair Information Practices[iii] endorsed by the FTC—notice, choice, access, security, and accountability—only notice can be said to be present as a result of privacy statements.

The first fluctuation in the FTC's commitment to self-regulation occurred in 1998, after the agency's survey of online practices showed that the lowest level of protection for consumer, notice of privacy practices, was not widely implemented. In a survey of 1400 web sites conducted by the Commission, 92% of the commercial sites collected personal information but only 14% had privacy notices. Of the commercial sites, only 2% had a "comprehensive" privacy policy.[iv] In reaction to these findings, the FTC was "still hopeful" that industry efforts would produce adequate privacy protections.[v] At the time, Chairman Pitofsky recommended that Congress pass legislation if self-regulation failed to produce significant progress.[vi]

A year later in testimony to Congress, the FTC renewed its faith in self-regulation, noting that many web sites had adopted privacy policies. But protections beyond mere disclosure of practices lagged behind. Only a small number of surveyed sites had incorporated choice, access, and security into their practices. No meaningful avenue for enforcement existed at all. Commissioner Sheila Anthony concurred with the report's findings but dissented from its recommendations, noting, "industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996. Notice, while an essential first step, is not enough if the privacy practices themselves are toothless. I believe that the time may be right for federal legislation to establish at least baseline minimum standards."

"Notice, while an essential first step, is not enough if the privacy practices themselves are toothless."

In 2000, a 3-2 majority of the FTC formally recommended that Congress adopt legislation requiring commercial web sites and network advertising companies to comply with Fair Information Practices.[vii] However, a year later with the appointment of a new FTC Chairman, the FTC embraced self-regulation again. Chairman Muris decided to focus the Commission's attention on enforcing existing laws rather than create new legislative protections for online privacy.[viii] Chairman Muris indeed has expanded privacy protections through the creation of a do-not-call list and

with application of the agency's powers to prevent unfair and deceptive trade practices.

The overall effect of the FTC's approach has been to delay the adoption of substantive legal protection for privacy. The adherence to self-regulatory approaches, such as the Network Advertising Initiative that legitimized third-party Internet tracking and the Individual References Service Group principles that concerned sale of SSNs, allowed businesses to continue using personal information while not providing any meaningful privacy protection. Ten years later, online collection of information is more pervasive, more invasive, and just as unaccountable as ever—and increasingly, the public is anesthetized to it.

It doesn't have to be this way. The FTC has been effective in protecting privacy when dealing with 20th century nuisances. It's time for the FTC to apply the lessons from telemarketing and other efforts to address the 21st century problem of Internet privacy.

III. Today's Tracking Methods Are More Pervasive and Invasive

Seven years ago, EPIC's report Surfer Beware I reviewed the status of Internet users' privacy rights and protections on the 100 most frequently visited web sites. The report was concerned primarily with the solicitation, collection, use, and protection of personal information obtained either from user-input forms or cookies.

Today, there are many more methods through which users can be tracked, profiled, and monitored in the online world. Cookie technology has matured—cookies are widespread and new uses have been developed. Entirely new technologies have emerged as well, some of which are all but unknown to consumers. Few of these methods are regulated, either internally by industry or externally by government. Without privacy legislation to protect Internet users from improper use of the information collected on the web, companies are unlikely to voluntarily cease privacy-invasive practices.

Cookies

Surfer Beware I discussed an Internet tracking technology over which there was "a great deal of controversy"—cookies. It found that about a quarter of the most frequently visited web sites used cookies. Today, many websites use cookies for one reason or another. In addition, there are several new wrinkles in the use of this tracking technology.

Third Party Cookies

Today, websites that a user explicitly visits are not the only entities which place cookies in your web browser—many web sites contain advertising served by outside commercial providers, and these providers may also send a cookie to your browser. These are known as "third party cookies." Some web browsers, such as Firefox allow users to block third party cookies.

Many web pages today have arrangements with third party ad servers that serve advertisements to their pages. For example, the MSN Privacy Statement lists two dozen third party ad networks that may place cookies in a user's browser.[ix]

Privacy policies (such as MSN's) tend to frame these third party cookies as a benefit to the user, allowing advertisers to "deliver targeted advertisements that they believe will be of most interest to you."

Persistent Cookies

A persistent cookie is one that remains on a user's computer after she has quit the browser. These cookies can be used to set and remember a user's web site preferences, settings, and passwords from one browser session to the next, but can also be used for

tracking and monitoring purposes. A troubling recent trend is to design these cookies to remain not just for many browser sessions, but for many years. Google's search cookie, for example, will not expire until January 17, 2038. This kind of long range tracking of users raises significant privacy risks.

Web Bugs

A web bug is a graphic on a web page that allows tracking and monitoring of visitors to that page. Web bugs are usually invisible, "clear" images only 1-by-1 pixel in size. They are capable of transmitting, back to the bug's originating server your Internet Protocol ("IP") address, the page you visited, the time you visited, browser information, and information from existing cookies in the browser.

For market approaches to work, consumers must grasp both technology and practices. But in a Pew Internet Report, 56% surveyed couldn't identify a cookie.[x]

Web bugs are sometimes used for the innocuous purpose of counting how many times a particular page is viewed and gathering statistics about browser usage and web site usage. There are, however, much more invasive uses, such as compiling a detailed web-browsing profile of a particular user.

Web bugs are designed specifically to be secret and invisible. Many Internet users today are aware of cookies, and may perceive them from the appearance of visible advertisements. There are also tools to manage cookies. Web bugs, however, can transmit information and set cookies even when there is no telltale banner advertisement on the website tipping off a user that information might be collected about them. Furthermore, just one "allowed" cookie from an ad network opens the door for all web bugs within that network to collect browsing information about that user. With companies such as DoubleClick, providing advertising to countless web sites, this risk is significant. For instance, if a user with a DoubleClick cookie in their browser loads a web page with a DoubleClick web bug on it, that bug can grab the identifying information in the cookie and transmit it back to the server along with the other information collected by the bug.

Google's Gmail Content Extraction

On April 1, 2004, Google announced the launch of their new Gmail service. Gmail is a web-based e-mail service offering one-gigabyte of e-mail storage to users. Gmail is supported by advertisers who buy keywords, much like the Google search engine's AdWords advertising program, which lead to targeted advertisements displayed alongside an e-mail message in a Gmail user's inbox. Gmail uses "content extraction" (a term from Google's patents) on all e-mails sent to and from a Gmail account in order to target the advertising to the user.

"If Google ogles your e-mail, will Ashcroft be far behind?"[xi]

Many privacy advocates hold the position that the Gmail service violates the privacy rights of both Gmail users and non-subscribers. Non-subscribers who e-mail a Gmail user have "content extraction" performed on their e-mail even though they have not consented to have their communications monitored, nor may they even be aware that their communications are being analyzed.

This is a significant development in Internet tracking technology because it is one of the first with the capacity and the structure to monitor and record not just transactional data

and personal information, but the content of private communications.

Spyware

Spyware and adware are extremely invasive and annoying technologies that have flourished in the self-regulatory world of Internet privacy. Both can be broadly described as pieces of software placed on a user's computer by a third party that perform unwanted functions. Spyware and adware collect information about the user, sometimes in complete secrecy without the knowledge of the user. Some programs display pop-up ads on the user's monitor, while others track and record everything the user does online. Information is sometimes collected by the programs for the sole purpose of sending that data back to an advertiser, and other times used to immediately serve pop-up ads to the user. Users often inadvertently download and install spyware and adware along with other desired computer programs, most commonly file-sharing applications. McAfee, an Internet security firm that sells popular virus protection and other personal computer security programs, reported more than 2.5 million "potentially unwanted programs" on its customers' computers, as of March 2004.[xii]

IV. More Invasive Tracking Mechanisms Are on the Horizon

There are several new and emerging technologies that have the potential to present significant privacy problems as they become more advanced and more widely used.

Digital Rights Management

Digital Rights Management (DRM) systems use technical means to protect an owner's interest in software, music, text, film, artwork, etc. DRM can control file access (number of views, length of views), altering, sharing, copying, printing, and saving, through either the software or hardware of a computer or device.

"Digital copyright management systems…are not some remote, futuristic nightmare…they will enable an unprecedented degree of intrusion into and oversight of individual decisions about what to read, hear, and view."[xiii]

Some DRM technologies are being developed with little regard for privacy protection. These systems require the user to reveal his or her identity in order to access protected content. Upon authentication of identity and valid rights to the content, the user can access the content. Widespread use of DRM systems could lead to an eradication of anonymous consumption of content.

DRM systems could lead to a standard practice where content owners require all purchasers of media to identify themselves. DRM can also link or tie certain content inextricably to one particular user. Windows Media Player, for example, has an embedded globally-unique identifier that can track users and the content they are viewing.

Trusted Computing

Trusted computing is a platform for pervasive DRM in personal computers. The Trusted Computing Group, an industry consortium with members Microsoft, Intel, Hewlett Packard, and Advanced Micro Devices, is overseeing the creation of industry-wide specifications for trusted computing hardware and software.

Trusted computing systems combine hardware and software elements to create a platform that gives software vendors an incredible amount of control over what users do with their computers. These systems have

been developed to protect the security of the computer from its owner when she uses proprietary or copyrighted information.

Computer freedom itself is at stake here. DRM can convert a flexible, user-controlled computer into an inflexible, copyright-owner-controlled surveillance device. Your next computer may really be a TV that watches you.

While trusted computing does enable a number of important security and privacy-enhancing functions, it also creates new threats to privacy and anonymity that should be seriously considered. For example, by augmenting the security functions already present on personal computers, trusted computing may offer greater protection from malicious programs or remote exploits. On the other hand, Trusted Computing could make it difficult or impossible for users to access content anonymously.

As trusted computing technology develops, it could have significant impact on computer users' privacy in the digital and online world.

Single Sign On Services

"Project Liberty" is an online identification and authentication system. It allows individuals to use a single sign-on in order to access many different web pages, and is being developed by a coalition of companies. A similar system has been designed by Microsoft, known as Passport or .NET Passport.

Identification and authentication systems present privacy risks for individuals. They can become virtual tollbooths for the Internet, requiring identity before one can view web pages. This violates a fundamental principle of privacy—the idea of collection limitation. It is illegitimate to collect information unless it is actually necessary to complete some function. However, with a proliferation of authentication systems, it becomes easier to compel individuals to identify themselves for no legitimate reason. These systems also enable profiling, which results in more spam, direct mail, and telemarketing for individuals.

V. The Privacy Friendly Are Mimicking the Privacy Invasive

In Surfer Beware I, EPIC noted that news web sites usually did not require disclosure of personal information in order to access their content, a practice that enhances privacy. The report stated that many of the top web sites allow "users to visit without giving up personal information. Anonymity plays a particularly important role for those sites…that are providing news and information to the on-line community." EPIC thought that it was especially appropriate for news sites not to attempt to identify site visitors, as anonymous access to political information shields individuals from law enforcement scrutiny and politically-motivated retribution.

But the ability to view the news anonymously is dramatically limited now. More and more news websites are requiring disclosure of personal information in various forms in order to access news articles.

EPIC conducted a survey of the websites of the top twenty-five US newspapers (by daily circulation).[xiv] Thirteen of these top twenty-five sites require disclosure of some personal information in order to access content. Seven newspapers (including three of the top five) actually require "registration." All seven of these sites require disclosure of personally identifiable information. The other five sites require only disclosure of information which is not, on its own, personally identifiable (gender, postal code/country, and birth year).

Internet users are becoming increasingly frustrated with the prevalence of registration requirements on Internet sites. Evidence suggests that users will go out of their way to avoid divulging personal information on news sites. Many users who don't want to divulge personal information in order to read the news online are engaging in "privacy self defense," as they enter false information in registration pages, or turn to services such as Bugmenot.com. Bugmenot is a website through which users can "share" personal login information, and as of August, 2004, claims to have "liberated" more than 18,000 pages from the confines of required registration.

Online users have strong reservations about the use and abuse of their personal information. Surveys show that people value anonymity, especially on the Internet, and simply don't want to give up their information.

A 2003 Annenberg Survey found that 57% of those polled believed that if a company has a privacy policy, the company will not share information with other entities.[xv]

The mere existence of a "privacy policy" also does not ensure that a person's information will remain "private" in the common sense of the word—both the LA Times and Chicago Tribune websites do not allow users to opt out of information sharing, advertising and communications from the newspapers and their "affiliates" (although you can opt out of sharing of your information with their advertisers and other third parties). There is also some indication that some newspapers have been checking the data provided at registration against third party commercial databases for accuracy.[xvi]

Compulsory site registration is likely to become a "vicious cycle" of privacy violations—increasing prevalence of privacy self-defense through providing "bad" or incorrect information might result in an increased tendency on the part of newspapers to require more invasive information from users, and to compare this information to commercial databases to ensure accuracy.

VI. Previous Self-Regulatory Initiatives Have Failed

Instead of driving towards legally accountable privacy frameworks, the FTC has a predilection towards self-regulatory initiatives. One notable effort was the NAI—The Network Advertising Initiative. The NAI was announced in 1999 shortly after DoubleClick, an online target advertising company, was the subject of a FTC investigation. The investigation was spawned by reports that the company was planning to link its anonymous surfing data with detailed offline customer profiles from Abacus Direct. Public protest led them to suspend their plans to merge their anonymous data with the personal information they had purchased.

Strong public opposition to online profiling caused Congress and the FTC to make efforts to address the practice. In November 1999, the FTC and Department of Commerce announced the formation of the NAI at a Workshop on Online Profiling. Less than a year later and with little involvement from consumer and privacy groups, the self-regulatory NAI principles were publicized.

The NAI standards were too weak to provide privacy commensurate with surfers' expectations. They encompassed only notice, opt-out, and "reasonable" security. NAI members could transfer information amongst themselves to an unlimited degree, so long as

it is used for advertising. No meaningful enforcement mechanism was incorporated.

Even where the NAI set privacy standards, they were burdensome for individuals to exercise. For instance, users who didn't want to be tracked by DoubleClick's cookies had to download and leave an "opt-out cookie" in their browser. For those who think that deleting their cookies enhances their privacy protections, they will have to repeatedly remember to download the cookie.

Further contributing to the irrelevance of NAI is the fact that its membership has depleted to two: DoubleClick and Atlas DMT.

New Tracking Methods Undermine the Already Weak NAI Provisions

Behavioral targeting is becoming increasingly popular with web ads that follow users as they browse the web. These ads can be targeted to a visitor's online habits. Many of these ads rose in popularity from keyword searches, however, more omniscient tactics are also at work. Revenue Science, for instance, offers their customers web bugs to collect user information. Individual sites can determine which data gets used for targeting and the information collected does not get shared among different sites using the service. Customers of Revenue Science include ESPN, Reuters, Dow Jones, Newsweek, The Wall Street Journal and many others.

As more network advertisers benefited from electronic espionage, the relevancy of the NAI dwindled as the two member companies no longer controlled the industry. Companies such as Google, Overture, Aquantive and Omniture are all influential stakeholders in the targeted advertising market and profiling business. Although they are not NAI members, the common theme of self-regulation has remained popular. Not surprisingly, the core of the weak NAI principles can still be identified throughout the privacy policies of the major network advertisers.

The NAI Principles Didn't Provide Privacy Then and Don't Provide it Now

The NAI principles have not contributed to an environment where privacy is protected. Only notice has effectively been conveyed online. Although consent varies depending on opt-out/opt-in policies, most advertisers operate on a no consent or opt-out model. While access is often provided for, a user is often only given access to the information that they have voluntarily provided to the company. However, in order for meaningful access to be attained, a user must able to receive the same electronic profile that is of value to the marketer. Accountability and enforcement are equally meaningless concepts without a central authority to monitor and impose the standards. Without enforceable rights, Internet users will continue to be tracked and profiled as they become pawns of the advertising industry.

IRSG: Freeing the Commercial Data Brokers From Privacy Responsibilities

The Individual Reference Services Group (IRSG) Principles were developed by commercial data brokers in the late 1990s in order to manage fomenting criticism regarding their business model. These data brokers sold Social Security Numbers and detailed dossiers on Americans to marketers, insurers, private investigators, landlords, and law enforcement.

The IRSG Principles set forth a weak framework of protections. They allowed companies to sell non-public personal information "without restriction" to "qualified subscribers." The problem is that everyone with an account is "qualified."

Under the IRSG Principles, individuals can only opt-out of the sale of personal information to the "general public," but commercial data

brokers don't consider any of their customers to be members of the general public. For instance, data broker ChoicePoint gives individuals no right to opt out and claims that "We feel that removing information from these products would render them less useful for important business purposes, many of which ultimately benefit consumers."

The IRSG Principles have been carefully crafted in order to ensure maximum flexibility for data brokers. They represent another self-regulatory failure that has resulted in easy access to detailed dossiers on Americans by both commercial and law enforcement interests. By turning a blind eye to the commercial sector, Congress allowed commercial data brokers to become "Big Brother's Little Helpers." They have created a national data center of personal information for law enforcement.[xvii]

NAI and IRSG Were Successful—For Those Invading Privacy

These self-regulatory initiatives served their purpose—to stop Congress from creating real, enforceable rights while allowing privacy-invasive activities to continue. They placated the FTC, causing Congress not to act. The end result has been that the FTC hasn't taken action to address traditional network advertisers or newer forms of privacy invasive tracking. Similarly, since Congress didn't act on data brokers, the IRSG has dissolved, and its member companies continue to sell personal information widely.

VII. Anonymous Purchasing Options: Another Market Failure

Even if a given online retailer extends strong privacy protections to customers, popular payment methods are not anonymous and provide an avenue for online profiling. Credit card companies use and sell personal information for target marketing, and provide an easy trail for law enforcement access to purchasing information.

Currently, there are not ubiquitous and easy to use anonymous online purchasing mechanisms. Companies in recent years have offered anonymous purchasing services based on various models, but these approaches tend to be cumbersome and costly.

In testimony to Congress in 1997, the Federal Trade Commission discussed anonymous payment systems and recommended that: "federal government should wait and see whether private industry solutions adequately respond to consumer concerns about privacy and billing dispute resolution issues that arise with the growth of electronic payment systems, and then step in to regulate only if those efforts -- be they market-created responses, voluntary self-regulation or technological fixes, or some combination of these -- are inadequate…"[xviii] How much longer does the consumer have to wait for user-friendly, ubiquitous anonymous payment options?

VIII. Information [In]Security

One of the five fair information practices endorsed by the FTC is security—the responsibility that data collectors take reasonable steps to assure that information collected from consumers is secure from unauthorized use.[xix]

Collection of personal information creates security risks for individuals. As companies amass personal information or send it elsewhere for processing, the databases become attractive targets for malicious actors.

It is difficult for individuals to assess the security and integrity of data collectors' systems. And recent events indicate that security in the data collection and processing industries falls fall short of being "reasonable."

A recent case in point involves Acxiom, a publicly-traded corporation that sells personal data and processes it for client companies. In a written statement to the FTC in June 2003, Acxiom's CEO assured that its security practices were "exceptional" and multi-leveled: "…it must be noted that Acxiom undertakes exceptional security measures to protect the information we maintain…and around the information we process for our clients to ensure that information will not be made available to any unauthorized person or business…"[xx]

A month after making this statement, Acxiom was informed by law enforcement officials that an Ohio man was able to download and crack Acxiom's password database. The method of stealing the personal information shows that Acxiom did have extraordinary security measures—the problem was that they were extraordinarily sloppy. The man, using FTP access operated for Acxiom's clients, was able to browse around Acxiom's system and download a single file containing all the passwords.[xxi] In the course of the Ohio investigation, Acxiom learned that a second man used the same technique to access over 8 gigabytes of personal information from April 2002 to August 2003.[xxii]

And, while the SSNs and credit card numbers of 20 million were accessed, the identities of companies that provided the personal information to Acxiom remain secret.

Acxiom did have extraordinary security measures—they were extraordinarily sloppy.

Other indications of information insecurity abound thanks to a California law that took effect in July 2003. That law requires data collectors to notify individuals when their data has been stolen. As a result, the public has heard of many information security breaches that normally would have been kept secret.

The first publicized notice of a security breach involved a banking consultant who had financial details on his computer. An office burglar stole the computer, which had credit line information, Social Security Numbers, and other bank account information.[xxiii] Since then, news of security breaches routinely appear in the national media.

IX. Bad Online Practices Are Leeching into the Offline World

The trend of collecting personal information and monitoring purchase habits is not strictly limited to the on-line environment. Increasingly, merchants are requiring consumers to produce identification or reveal personal information at the point of sale or when they wish to return or exchange an item.

What's Your Phone Number?

Increasingly, cashiers are asking individuals for their phone numbers. This places individuals at risk that they will receive telemarketing based on the most trivial of purchases in the offline world.

Consumers don't realize that giving a phone number to a cashier invites telemarketing under the "established business relationship" loophole to the Telemarketing Do-Not-Call Registry.

But the problem extends beyond a cashier's request for information, rather, it is the presumption that the disclosure of personal information has become a precondition of sale. While a customer may feel uneasy about revealing this information, many do not know that this disclosure is voluntary. And because

individuals want to shield their personal information from disclosure, some data companies have developed stealth information collection techniques for offline retailers. For instance, Trans Union, a credit reporting agency, offered "Translink / Reverse Append," a product that gave retailers name and address information from credit card numbers collected at the register.[xxiv] Consumers are not actually asked for their address, and probably are not aware that their address is discoverable.

The exact purpose for this information collection varies from store to store. Nine West asks for customer information in order to create a database of transaction histories for each customer, containing shoe size and width. Victoria's Secret has recently begun asking customer's for their telephone numbers so that they may be informed of promotions. Sometimes, it is difficult to find out how the information is being used.

Grocers Get Loyalty and We Get Less

Frequent shopper or loyalty card programs vary depending on the type of retailer or service. Generally, grocery stores will offer loyalty cards where a customer reveals a significant amount of personal information in exchange for a card which makes them eligible for in-store discounts. There is a high privacy risk associated with these cards as a great deal of personal data is revealed and all purchased are tracked.

Consumers are led to believe that they saving money when in reality, the prices at non-savings card stores are often lower.

A 2003 Wall Street Journal study found that "most likely, you are saving no money at all [from supermarket shopping cards]. In fact, if you are shopping at a store using a card, you may be spending more money than you would down the street at a grocery store that doesn't have a discount card."[xxv]

The Wall Street Journal reported that, "…according to industry experts…[loyalty] cards are designed to make customers feel like they got a bargain, without actually lowering prices overall."

The Wall Street Journal study surveyed card and non-card grocery stores in five different American cities and concluded that "In all five of our comparisons, we wound up spending less money in a supermarket that doesn't offer a card, in one case 29% less."[xxvi] The author further wrote that "…according to industry experts, our shopping experience was typical, because cards are designed to make customers feel like they got a bargain, without actually lowering prices overall. 'For many customers, the amount of money saved has not risen,' says Margo Georgiadis, a specialist in loyalty programs at McKinsey & Co. The difference is that stores now make you carry a card to get the discounts, whereas before they just offered plain old sale prices."[xxvii]

Making a Return? Your Papers Better Be in Order

A review of the return policies of select retailers indicates that asking for identification for returns, even when an original receipt is present, is becoming a common practice. In some situations, this requirement is even printed on the receipt while other merchants fail to post any notice of this condition. While some retailers simply take the identification to match the name and contact information, others go as far as to enter the driver's license number into their computer system. Often, a customer might not even know that this is

occurring, or they may feel as though the recording of their driver's license number is a necessary step. Given the sensitivity of the information contained on a driver's license, when combined with credit card information that is often available at a return, this practice places the customer at risk of identity theft.

Consumer Returns Database

Some point of sale return information is being added to a little-known system known as the "Consumer Returns Database."[xxviii] The database is offered by The Return Exchange which offers a standardized return system to retailers. It operates in real-time by monitoring consumer return patterns it helps merchants identify fraudulent or abusive customers.

It is unclear what standards are applied to identify an abusive customer, or the rights that a customer has to access and correct the database. A list of the retailers who participate in the database is not publicly available. By the time a customer is aware that negative information exists about them in the database, it is because they have already been branded as a fraudulent or abusive returner.

Firing the Customer

Combined, collection of returns information and loyalty behavior can tip the balance of power between the consumer and the retailer. Left unchecked, this data will be used for customer exclusion. As the Boston Globe recently put it, slow service or unattractive prices are being used "as a behavior modification tool to transform an unprofitable customer into either a profitable customer or a former customer."[xxix]

There is a growing movement in the "customer relationship management" or profiling industry where businesses are encouraged to eliminate customers who complain or who return goods. Jim Dion, president of retail consulting firm Dionco Inc., recently urged storeowners to create disincentives for certain customers.[xxx] Dion characterized 20% of the population as "bottom feeders," who complain and have low-levels of loyalty. Businesses, he argues, should try to eliminate these customers: "It'd be cheaper to stop them at the door and give them $10 not to come in."[xxxi] An article in DMNews quotes Dion as suggesting that retailers "should consider a preferred-customer database—prefer that they don't shop here."[xxxii]

"Filene's banned two sisters from all 21 of its stores last year after the clothing chain's corporate parent decided they had returned too many items and complained too often about service."[xxxiii]

And major businesses are adopting these recommendations. Best Buy's consumer exclusion tactics were recently detailed by the Wall Street Journal. Literally, Best Buy is trying to eliminate its most savvy customers, ones that recognize good deals, in favor of less thrifty customers that the company can charge more.[xxxiv] Other companies engage in consumer exclusion in more subtle ways, for instance, Harrah's casinos automatically identifies callers and charges them for hotel rooms based on their perceived profit potential.[xxxv] The company hides the profiling system because consumers, if fully informed, would find the practices creepy.

First-Degree Price Discrimination

"First-degree price discrimination," a practice where businesses attempt to "perfectly exploit the differences in price sensitivity between consumers," is a growing problem resulting from collection of consumer information.[xxxvi] As Professor Janet Gertz has explained: "By profiling consumers, financial

institutions can predict an individual's demand and price point sensitivity and thus can alter the balance of power in their price and value negotiations with that individual. Statistics indicate that the power shift facilitated by predictive profiling has proven highly profitable for the financial services industry. However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers. For this reason, and because most consumers have no practical ability to negotiate price terms for the exchange of their data, many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure."[xxxvii]

First-degree price discrimination is a goal of some in the information business. CIO Insight Magazine recently published an article discussing pricing ceilings where price discrimination is described as a goal for the industry: "The ideal strategy? To capture the value of the product or service for a particular customer or customer segment."[xxxviii]

X. Recommendations

The FTC has to move into the 21st century and meaningfully address Internet privacy. Ten years of self-regulation has led to serious failures in this field. The online privacy situation is getting worse, so bad that offline retailers are emulating the worst Internet practices.

The FTC certainly is capable of protecting privacy online. It has to rise to the challenge and exercise more skepticism in the market as a proxy for consumer interest. Sometimes the market advances consumer interests, but when it comes to privacy, the market has been a driving force in eroding both practices and expectations. In order to rise to the challenge of effectively protecting individuals' privacy, we recommend the following:

- The FTC should abandon its faith in self-regulation. Self-regulatory systems have served to stall Congress while anesthetizing the public to increasingly invasive business practices. Self-regulation has only been reliable in promoting privacy notices, the least substantive aspect of privacy protection. The public's, and even the FTC's own conception of Fair Information Practices, commands a broader array of privacy protection including access, choice, security, and accountability.
- The FTC should reexamine the Network Advertising Initiative in light of the agreement's dwindling membership and the existence of new, more invasive tracking measures.
- The FTC should reexamine the IRSG Principles to ensure that they provide some measure of meaningful privacy.
- The FTC should investigate the emerging technologies identified in this report, including digital rights management, trusted computing, and single sign on services.
- The FTC should investigate the emerging offline business practices identified in this report, including unnecessary requests for information at point of sale or return, customer return databases, customer exclusion, and first degree price discrimination.
- The FTC should work with the banking agencies to develop a unified mechanism for opting out under the Gramm-Leach-Bliley and Fair Credit Reporting Acts. Just as it made no sense for individuals to opt-out of every telemarketing call, it currently makes no sense for an individual to have to contact every single financial institution separately to protect privacy.

*This report was written with assistance from EPIC Internet Public Interest Opportunity Program (IPIOP) Clerks Dina Mashayekhi, Tara Wheatland, and Amanda Reid.

[i] *Consumers deserve stronger shield against telemarketers*, USA TODAY, Sept. 17, 2002. In just one year, the New York DNC list amassed 2 million enrollments. *Telemarketing's Troubled Times*, CBS NEWS, Apr. 1, 2002, at http://www.cbsnews.com/stories/2002/04/01/eveningnews/main505124.shtml.

[ii] *Self Regulation and Privacy Online, Before the House Commerce Subcomm. on Telecom., Trade, and Consumer Protection*, 106th Cong., Jul. 13, 1999, available at http://www.ftc.gov/os/1999/07/pt071399.htm.

[iii] FTC, STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE, Dec. 1996, available at http://www.ftc.gov/reports/privacy/privacy1.htm.

[iv] FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, Jun. 4, 1998, available at http://www.ftc.gov/reports/privacy3/index.htm.

[v] FTC, SELF-REGULATION IS THE PREFERRED METHOD OF PROTECTING CONSUMERS' ONLINE PRIVACY; Jul. 21, 1998, available at http://www.ftc.gov/opa/1998/07/privacyh.htm.

[vi] *Consumer Privacy on the World Wide Web, Before the House Comm. on Commerce Subcomm. on Telecommunications, Trade, and Consumer Protection*, 105th Cong. (Jul. 21, 1998) (statement of the FTC), available at http://www.ftc.gov/os/1998/07/privac98.htm.

[vii] FTC, ONLINE PROFILING:A REPORT TO CONGRESS PART 2 RECOMMENDATIONS, Jul. 2000, available at http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

[viii] Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Remarks delivered at the Privacy 2001 Conference, Oct. 4, 2001, available at http://www.ftc.gov/speeches/muris/privisp1002.htm.

[ix] Ad4Ever; AdCentric Online; Ad Dynamix; AdSolution; Avenue A; BlueStreak; BridgeTrack; DoubleClick; efluxa; Enliven; Flycast; i33; Mediaplex; PlanetActive; Pointroll; Profero; Qksrv; RealMedia; RedAgency; TangoZebra; TargetGraph; TrackStar; Travelworm; Unicast.

[x] PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES, Aug. 20, 2000.

[xi] *Company Needs to Engage Privacy Advocates in a Thorough Debate*, SAN JOSE MERCURY NEWS, Apr. 15, 2004.

[xii] David McGuire, *States Speed up Spyware Race*, WASH. POST, May 13, 2004, available at http://www.washingtonpost.com/wp-dyn/articles/A24746-2004May13.html

[xiii] Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (Summer 1996).

[xiv] BURRELLESLUCE, TOP 100 DAILY NEWSPAPERS IN THE U.S. BY CIRCULATION 2004.

[xv] Joseph Turow, *Americans and Online Privacy: The System is Broken*, Annenberg Public Policy Center, June 2003.

[xvi] Rachel Metz, We Don't Need No Stinkin' Login, Wired Jul. 20, 2004, available at http://wired.com/news/infostructure/0,1377,64270,00.html

xvii Chris Jay Hoofnagle, *Big Brother's Little Helpers*, 29 N.C.J. INT'L L. & COM. REG. 595 (Summer 2004).

[xviii] FTC, WAIT, WATCH CLOSELY AND SEE IS RIGHT STANCE FOR GOVERNMENT ON PRIVACY ISSUES FOR ELECTRONIC PAYMENT SYSTEMS, SAYS FTC OFFICIAL, Sept. 18, 1997, available at http://www.ftc.gov/opa/1997/09/medine.htm.

[xix] FTC, ONLINE PROFILING:A REPORT TO CONGRESS PART 2 RECOMMENDATIONS, Jul. 2000, available at http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

[xx] Information Flows, Before the FTC, Jun. 18, 2003, available at http://www.ftc.gov/bcp/workshops/infoflows/present/030618morgan.pdf.

[xxi] Robert O' Harrow, Jr., NO PLACE TO HIDE 71-72, Free Press (2005). DOJ, MILFORD MAN PLEADS GUILTY TO HACKING INTRUSION AND THEFT OF DATA COST COMPANY $5.8 MILLION, Dec. 18, 2003, available at http://www.usdoj.gov/criminal/cybercrime/baasPlea.htm.

[xxii] DOJ, FLORIDA MAN CHARGED WITH BREAKING INTO ACXIOM COMPUTER RECORDS, Jul. 21, 2004, available at http://www.usdoj.gov/opa/pr/2004/July/04_crm_501.htm.

[xxiii] *Customer Data Was on Stolen PC, Wells Fargo Says*, Reuters, Nov. 21, 2003.

[xxiv] *In re Trans Union*, 2000 FTC LEXIS 23 (2000).

[xxv] Katy McLaughlin, *The Discount Grocery Cards That Don't Save You Money*, Wall Street Journal, Jan. 21, 2003, at http://wsj.com/article/0,,SB1043006872628231744,00.html.

[xxvi] *Id*.

[xxvii] *Id*.

[xxviii] http://www.thereturnexchange.com/

[xxix] Bruce Mohl, *Facing their demons: To face demons, firms dump maxim*, BOSTON GLOBE, Jul. 27, 2003.

[xxx] Mickey Alam Khan, *Technology Creates Tough Environment for Retailers*, DMNews, Jan. 13, 2003.

[xxxi] *Id*.

[xxxii] *Id*.

[xxxiii] Joshua Freed, *The customer is always right? Not anymore*, SAN FRAN. CHRON., Jul. 5, 2004.

[xxxiv] Gary McWilliams, *Analyzing Customers*, WALL STREET JOURNAL, Nov. 8, 2004.

[xxxv] Christina Binkley, *Taking Retailers' Cues, Harrah's Taps Into Science of Gambling*, WALL STREET JOURNAL, Nov. 22, 2004.

[xxxvi] Anthony Danna & Oscar H. Gandy, Jr., *All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining*, 40 JOURNAL OF BUSINESS ETHICS 373, 381 (2002).

[xxxvii] Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 964-5 (Summer 2002).

[xxxviii] Amy Cortese, *Price Flexing: How the Web Adds New Twists*, CIO Insight, at http://www.cioinsight.com/article2/0,3959,43528,00.asp.

Maxim

Published by Dennis Publishing, Maxim is the essential guidebook for young men.

Key Segments

1,743,000	Universe / Base Rate	$105.00 /M
1,327,000	Total Male Subs	+ $8.00 /M
129,000	Total Female Subs	+ $8.00 /M
600,000	6 Month Subs	+ $6.00 /M
314,000	3 Month Subs	+ $11.00 /M
117,000	1 Month Subs	+ $16.00 /M
128,000	Change of Address	+ $11.00 /M
36,000	Canadian	+ $21.00 /M
	Catalog Rate	$85.00 /M
	Fundraiser Rate	$75.00 /M

Audience Profile

Riding a wave of extraordinary popularity Maxim became the world's largest circulation men's magazine by addressing the real life needs of intelligent, professional men in an entertaining as well as informative way. One of the most talked about magazines in America since its launch in 1997, Maxim reaches men age 18-34, the time in their lives when it all comes together—careers, recreation, relationships.

LIST TYPE
Consumer mail

SOURCE
Direct mail sold

GEOGRAPHY
Domestic (US) and Canada

LIST OWNER
Dennis Publishing

LIST MAINTENANCE

New to ALC	12/01/2002
Counts through	06/30/2004
Last update	07/13/2004
Update frequency	MONTHLY

UNIT OF SALE INFORMATION
Average: **$17.94**

GENDER PROFILE

Male:	**77%**
Female:	**7%**

INCOME
Average: **$65,000.00**

SELECTION CHARGES

1 MONTH HOTLINE	$16.00 /M
3 MONTH HOTLINE	$11.00 /M
6 MONTH HOTLINE	$6.00 /M
BUSINESS ADDRESS	$11.00 /M
CHANGE OF ADDRESS	$11.00 /M
GENDER/SEX	$8.00 /M
KEYING	$3.50 /M
PAID	$8.00 /M
SCF	$8.00 /M
SOURCE	$8.00 /M
STATE	$8.00 /M
ZIP	$8.00 /M

ADDRESSING

Reader's Digest provides an enriching breadth of editorial tha meets subscribers' insatiable appetite for service journalism, current events, humor, and adventure that stem from The Digest's core affinities-health, home, family, finance, and faith.

Key Segments

5,111,000	Universe / Base Rate	$95.00
2,619,000	Active Female Subscribers	+ $8.00
2,149,000	Active Male Subscribers	+ $8.00
1,329,000	3 Month Hotline	+ $10.00
230,000	1 Month Hotline	+ $15.00
67,400	1 Month Change of Address	+ $15.00
1,789,000	Sweeps Sold Subscribers	+ $15.00
1,390,000	Gift Givers for Nonpub. Mailers	$100.00
	Catalog Rate	$80.00
	Fundraiser Rate	$75.00
	(enhancements are available, please inquire)	

NEWSWEEK CATHOLIC SUBSCRIBERS

DMI#: 47610
MIN#: 10973 SRDS#: 52860

416,634 Catholic Subscribers $95/M
Counts are through June 2004

DESCRIPTION:
Newsweek has identified the Catholic subscribers with InfoBase lifestyle and demographic information. Newsweek Catholic subscribers not only respond to Catholic appeals but to a variety of other fundraising and non-profit organizations dedicated to humanitarian, cultural and health causes.

CURRENCY: US Dollars

GENDER:
Male: 64% Female: 36%

UNIT OF SALE:
$41.08/Year (52 Issues)

SELECTIONS:
$16.00/M 1-2 Month Hotline
$11.00/M 3-5 Month Hotline

HEARST MAGAZINES INTERNET SUBS AT POSTAL ADD

DMI#: 31444
MIN#: 70879

366,792 Active Subscribers $130/M
83,348 3 Month Hotline Subscribers ADD $15/M
Counts are through June 2004.

DESCRIPTION:
These consumers have visited the Hearst Magazine's websites and subscribed to one of their magazines via the internet. These names are available on a one-time use basis and are at home addresses.

Hearst Magazines combined all ten Hearst titles: Cosmopolitan, Country Living, Country Living Gardener, Esquire, Harper's Bazaar, House Beautiful, Good Housekeeping, Popular Mechanics, Redbook, and Town & Country to offer their internet generated subscribers.

CURRENCY: US Dollars

GENDER:
Male: 15% Female: 72%

SELECTIONS:
$15.00/M 3 Month Hotline
$10.00/M Age
$7.00/M Gender/Sex
$10.00/M Income
$7.00/M Paid
$10.00/M Parents of Children
$10.00/M Parents of Children by Age
$10.00/M Publication Title
$7.00/M SCF

PLANETOUT.COM

Data Verified: Dec 4, 2002.

Location ID: 10 DCLS 551 — Mid 648374-000

1. PERSONNEL
List Manager — Mal Dunn Associates, South Patterson Business Park East, 2022 Route 22, Brewster, NY 10509. Phone 845-278-1200. Fax 845-278-1300.
URL: http://www.dunndirect.com
Key Contact: Jennifer Schmidt, Phone 845-278-1339.

2. SUMMARY DESCRIPTION
Members of PlanetOut, an online community for gay, lesbian, bisexual and transgender individuals.

3. LIST SOURCE
Internet/online/website registration.

4. SELECTIONS WITH COUNTS
Updated: Dec 4, 2002.

	Total Number	Price per/M
Total list	178,570	115.00
Personal buyers	5,555	+5.00
Entertainment customers	48,053	"
Travel subscribers	63,100	"

4A. OTHER SELECTIONS
Gender, state, 5.00/M extra; SCF, 7.50/M extra; Zip, 10.00/M extra; age, 15.00/M extra; key coding, 3.00/M extra.

5. COMMISSION, CREDIT POLICY
20% commission to brokers. 15% commission to agencies. Payment due 30 days after mail date. Cancel charges: Cancellations must be in writing and accompanied by the returned names and are subject to running charges. Orders cancelled after mail date on purchase order will be charged full price.

6. METHOD OF ADDRESSING
Cheshire labels, 4-up, 1.00/M extra; pressure sensitive labels, 12.50/M extra; mag tape, 25.00 fee.

VICTORIA'S SECRET INTERNET BUYERS AT POSTAL ADDRESSES

Data Verified: Dec 12, 2002.

Location ID: 10 DCLS 544 — Mid 748415-000

1. PERSONNEL
List Manager — ClientLogic Specialists Marketing Services, 1200 Harbor Blvd., 9th Fl., Weehawken, NJ 07087. Phone 201-865-5800. Fax 201-867-2450.
URL: http://www.clientlogic.com
E-mail: listinfo@clientlogic.com
Key Contact: Kathy Hermann
E-mail: kathyher@clientlogic.com

2. SUMMARY DESCRIPTION
Victoria's secret internet buyers at postal addresses.
14% male, 80% female.
Average unit of sale 110.00.

3. LIST SOURCE
Direct mail, internet/online/website registration.

4. SELECTIONS WITH COUNTS
Updated: Dec 12, 2002 — Counts Thru: Nov 2002

	Total Number	Price per/M
Buyers (12 month)	1,574,316	*130.00
6 month	844,555	+11.00
3 month	457,360	+21.00
1 month	217,413	+41.00

(*) Fundraiser rate, 70.00/M; food rate, 75.00/M; publisher rate, 80.00/M.
Minimum order 10,000.

4A. OTHER SELECTIONS
SCF, Zip, state, 6.00/M extra; identifiable female/male, 7.50/M extra; sale buyers, non-sale buyers, 16.00/M extra; new to file, dollar type, dollar amount (25.00+), 11.00/M extra; 50.00+, 21.00/M extra; 75.00+, 26.00/M extra; 100.00+, 31.00/M extra; 150.00+, 41.00/M extra; 200.00+, 43.00/M extra; product type:; lingerie, ready to wear, shoes, handbags and accessories, denim, cosmetics/perfume, hosiery, sleepwear, bodywear, sportswear, petite buyers, 16.00/M extra; book type:; core, swim book, lookbook, shoe & accessory book, 16.00/M extra.

5. COMMISSION, CREDIT POLICY
Cancel charges: Orders cancelled after mail date will be charged full rental. Orders received and processed will be subject to a 50.00 flat cancellation fee and running charges.

6. METHOD OF ADDRESSING
E-mail, 75.00 fee; cartridge, 25.00 fee.

11. MAINTENANCE
Updated 12 times per year.

DISH WISH

Data Verified: Oct 19, 2002.

Location ID: 10 DCLS 521A — Mid 755119-000
Member: D.M.A.

1. PERSONNEL
List Manager — Great Lakes List Management, Inc., 3126 Peach Street, Erie, PA 16508. Phone 814-456-2175. Fax 814-455-1942.
URL: http://www.greatlakeslists.com
E-mail: info@greatlakeslists.com

2. SUMMARY DESCRIPTION
Responders to an internet solicitation via banner ads/email offering a satellite dish package, but credit approval was denied.

3. LIST SOURCE
Internet/online/website registration.

4. SELECTIONS WITH COUNTS
Updated: Feb 19, 2002.

	Total Number	Price per/M
Total list	10,000	75.00
Hotline (monthly)	7,500	+10.00

Minimum order 5,000.

4A. OTHER SELECTIONS
Zip+4, 2.50/M extra; title address, carrier route presort, geography, 5.00/M extra; gender, 10.00/M extra; phones, 75.00/M

CREDIT REPAIR FROM THE WEB

Data Verified: Sep 11, 2002.

Location ID: 10 DCLS 525 — Mid 748422-000

1. PERSONNEL
List Manager — Carney Direct Marketing, 15520 Rockfield Blvd., Suite C, Irvine, CA 92618. Fax 949-581-4564. Phone 949-581-5100.
URL: http://www.carneydirect.com

2. SUMMARY DESCRIPTION
Credit card seekers who were surfing the net in search of credit repair information.
55% male, 45% female.

3. LIST SOURCE
Telemarketing.

4. SELECTIONS WITH COUNTS
Updated: Sep 11, 2002.

	Total Number	Price per/M

DINING OUT KIDS BIRTHDAY CLUB

Data Verified: Sep 5, 2002.

Location ID: 10 DCLS 520 — Mid 103081-000

1. PERSONNEL
List Manager — Carney Direct Marketing, 15520 Rockfield Blvd., Suite C, Irvine, CA 92618. Fax 949-581-4564. Phone 949-581-5100.
URL: http://www.carneydirect.com

2. SUMMARY DESCRIPTION
Families with children ages 0-12 who fill out birthday club cards at a national restaurant chain.
Ages 0-14.

3. LIST SOURCE
Compiled retail records, warranties and, direct response questionnaires.

4. SELECTIONS WITH COUNTS
Updated: Sep 5, 2002.

	Total Number	Price per/M
Restaurant birthday members	1,075,088	75.00
Hotline	45,822	85.00

Minimum order 5,000.

4A. OTHER SELECTIONS
State, SCF, Zip, gender, of child, child name, 5.00/M extra; parents slug-in, 3.00/M extra; exact age, 15.00/M extra; key coding, 2.00/M extra.

5. COMMISSION, CREDIT POLICY
20% commission to brokers.

6. METHOD OF ADDRESSING
Cheshire labels, 4-up; pressure sensitive labels, 10.00/M extra; mag tape, 25.00 fee; diskette, 35.00 fee; e-mail, 50.00 fee.

8. RESTRICTIONS
Two sample mailing pieces required.

CYBER ENTERTAINMENT NETWORK

Data Verified: Jan 3, 2003.

Location ID: 10 DCLS 568 — Mid 607113-000

1. PERSONNEL
List Manager — Creative List Marketing, Inc., 35 Kennard Road, Ste. 1, Mahopac, NY 10541. Phone 845-621-8555. Fax 845-621-5839.
E-mail: creativelm@aol.com

2. SUMMARY DESCRIPTION
Male buyers (on the web) of live sexually oriented movies, games and videos.
Average unit of sale 30.00.

3. LIST SOURCE
100% internet/online/website registration Internet advertising.

4. SELECTIONS WITH COUNTS
Updated: Jan 7, 2002.

	Total Number	Price per/M
Buyers (2001)	111,371	85.00
2000	118,548	80.00
Hotline (monthly)	20,000	90.00

Minimum order 5,000.

4A. OTHER SELECTIONS
State, SCF, Zip, gender, 5.00/M extra; key coding, 2.00/M extra; multibuyers, 5.00/M extra; phone numbers, 150.00/M extra.

5. COMMISSION, CREDIT POLICY
20% commission to brokers. Cancel charges: Orders cancelled after mail date require payment in full. All cancelled orders will be billed an additional flat fee of 50.00.

6. METHOD OF ADDRESSING
Cheshire labels, 4-up; pressure sensitive labels, 8.00/M extra; mag tape, 25.00 fee; E-mail address, 100.00/M extra.

8. RESTRICTIONS
Sample mailing piece required.

ACTIVE INTERNET GAMBLERS

Data Verified: Apr 25, 2002.

Location ID: 10 DCLS 549 — Mid 752090-000

1. PERSONNEL
List Manager — Pioneer Pacific List Marketing, Inc., 14724 Ventura Blvd., # 502, Sherman Oaks, CA 91403. Phone 818-783-7500. Fax 818-783-7600.
Key Contact: Michael Scher

2. SUMMARY DESCRIPTION
Internet gamblers who have made a minimum deposit with an online gambling institution.

3. LIST SOURCE
Internet/online/website registration.

4. SELECTIONS WITH COUNTS
Updated: Apr 25, 2002 — Counts Thru: Mar 2002

	Total Number	Price per/M
Gamblers (2001)	694,515	*85.00
Names (January 2002)	57,411	"
February	57,440	"
Hotline (March 2002)	57,496	95.00

(*) E-mail addresses, 200.00/M.
Minimum order 5,000.

4A. OTHER SELECTIONS
SCF, Zip, state, 5.00/M extra; key coding, 3.00/M extra.

5. COMMISSION, CREDIT POLICY
Payment due 30 days after mail date.

6. METHOD OF ADDRESSING
Cheshire labels, 4-up; pressure sensitive labels, 8.00/M extra; mag tape, 25.00 fee.

8. RESTRICTIONS
Two sample mailing pieces required.

11. MAINTENANCE
Updated monthly.

ONLINE CREDIT NOW

Data Verified: Nov 20, 2002.

Location ID: 10 DCLS 525 — Mid 741850-000
Member: D.M.A.

1. PERSONNEL
List Manager — NeWorld Marketing, LLC, 70 Hazel Mill Rd., Asheville, NC 28806. Phone 828-252-7496. Fax 828-252-8124.
URL: http://www.neworldmarketing.com
Key Contact: Tom Manning
E-mail: tmanning@neworldmarketing.com

2. SUMMARY DESCRIPTION
Credit seeking individuals have responded to one or more offers made available by OnlineCreditNow.com.
55% male; average age 40.

3. LIST SOURCE
Internet/online/website registration.

4. SELECTIONS WITH COUNTS

ETHNIC SEGMENTATION OF AMERICAN HOUSEHOLDS - ET

Ethnic TECHNOLOGIES, LLC

Data Verified: Nov 11, 2002.

Location ID: 10 DCLS 538 — Mid 625777-000

1. PERSONNEL
List Manager — Ethnic Technologies, LLC, 600 Huyler St, South Hackensack, NJ 07606. Phone 201-440-8923. Fax 201-440-2168. Toll Free 866-333-8324.
URL: http://www.ethnictechnologies.com
E-mail: info@ethnictechnologies.com
Key Contact: Natl Sales Mgr—Candace Kennedy
E-mail: candace@etechllc.com

2. SUMMARY DESCRIPTION
Database of households in every state.

3. LIST SOURCE
Compiled.

4. SELECTIONS WITH COUNTS
Updated: Nov 11, 2002.

	Total Number	Price per/M
African American	7,221,658	65.00
Unique African American	717,620	"
Afghani	1,138	"
African African	113,792	"
Albanian	6,574	"
Aleut	1,646	"
Algerian	1,384	"
Angolan	311	"
Arabic	383,499	"
Armenian	162,898	"
Ashanti	1,755	"
Austrian	373,039	"
Azerbejanian	867	"
Basque	474	"
Belgian	56,365	"
Bengali	352	"
Benin	345	"
Bhutanese	601	"
Bosnian	1,602	"
Botswanian	329	"
Bulgarian	18,947	"
Burkina Faso	304	"
Byelorus	4,348	"
Cameroon	529	"
Cent AF Rep	356	"
Chad	1,234	"
Chechnian	58	"
Chinese	1,084,354	"
Comoros Isle	130	"
Congo	858	"
Croatian	46,705	"
Czech	343,808	"
Danish	315,635	"
Djibouti	183	"
Dutch	1,730,654	"
Egyptian	13,637	"
English	36,008,087	"
Estonian	22,833	"
Ethiopian	25,372	"
Equat Guinea	826	"
Filipino	156,625	"
Finn	131,625	"
French	2,856,187	"
Gabon	235	"
Gambian	1,272	"
German	7,586,873	"
Georgian	2,099	"
Ghanian	13,189	"
Greek	348,575	"
Guinea-Bissea	745	"
Hausa	3,047	"
Hebrew	114,695	"
Hispanic	10,433,718	"
Hungarian	240,113	"
Icelandic	1,876	"
Indian & Hindu	435,310	"
Indonesian	2,086	"
Iraqi	339	"
Irish	8,691,833	"
Italian	4,193,306	"
Ivory Coast	2,436	"
Japanese	432,901	"
Jewish ethnic	2,810,476	"
Kazakh	226	"
Kenyan	7,356	"
Khmer	15,601	"
Korean	359,234	"
Kurdish	262	"
Kirghizstan	62	"
Kuwaiti	70	"
Laotian	26,508	"
Latvian	18,058	"
Lesotho	139	"
Liberian	514	"
Libyan	284	"
Lithuanian	57,328	"
Macedonian	359	"
Malawi	476	"
Malay	576	"
Mali	2,585	"
Manx	861	"
Moldavian	397	"
Mongolian	2,769	"
Morroccan	1,583	"
Mozambique	132	"
Myanmar	10,241	"
Namibian	680	"
Nipal	528	"
Niger	730	"
Nigerian	27,071	"
Norwegian	534,317	"
Pakistani	41,597	"
Persian	70,429	"
Polish	1,315,057	"
Portugeuse	291,283	"
Qatar	350	"
Romanian	57,272	"
Ruandan	133	"
Russian	297,341	"

ADULT WEE

Data Verified: Jan 18, 20

Location ID: 10 DCLS 568

1. PERSONNEL
List Manager — MDI (form
dian Trace #307, Weston,
Fax 561-362-6689.
E-mail: MDILists@aol.com

2. SUMMARY DESCRIPTIO
Subscribers who use their
sex via the internet.
95% male; average age 42
Average unit of sale 29.95

3. LIST SOURCE
Direct response.

4. SELECTIONS WITH CO
Updated: Feb 15, 2002

Buyers (last 12 month)
Hotline (monthly)
Phones (monthly)
(*)Flat price.
Minimum order 10,000.

4A. OTHER SELECTIONS
State, SCF, Zip, 5.00/M ex

5. COMMISSION, CREDIT
20% commission to broke
Payment due 30 days afte
ders cancelled before the
75.00 cancellation fee. Prep
ers.

6. METHOD OF ADDRESSI
Pressure sensitive labels, 8

8. RESTRICTIONS
One time use only.

SCHOLARSHIPS.C

Data Verified: Jun 27, 2

Location ID: 10 DCLS 521

1. PERSONNEL
List Manager — 24/7 Ma
NY 10001. Phone 212-23
URL: http://www.247realm
E-mail: advertising@247r
Key Contact: Senior List
212-231-7197.
E-mail: amy.gosman@24

2. SUMMARY DESCRIPTI
Students and parents vis
scholarship and financial
gible for.

3. LIST SOURCE
Internet/online/website reg

4. SELECTIONS WITH CO
Updated: Jun 27, 2002

Postal addresses
Hotline (Monthly)
Demographic:
High school students
College students
Graduate students
Trade/technical school s
Parents
Minimum order 8,000.

4A. OTHER SELECTIONS
Key coding, 3.00/M extra
extra; hotline (30 day), 1
25.00/M extra; ethnicity, h
interests, birth date, area
year, GPA, ACT/SAT/GE
loan status, organizations
college planning to attend
10.00/M extra.

5. COMMISSION, CREDIT
20% commission to broke
date. Cancel charges: All
flat fee of 250.00. Orders
payment in full.

EMACHINES FIR PURCHASERS @

Data Verified: Jul 17, 20

Location ID: 10 DCLS 558A

1. PERSONNEL
List Manager — America
way 1, CN 5219, Princet
5478. Fax 609-580-2810.
Key Contact: Mike Gural,
E-mail: mike.gural@amlis

2. SUMMARY DESCRIPTI
Buyers of PC's and intern

3. LIST SOURCE
Internet/online/website re

4. SELECTIONS WITH CO
Updated: Apr 3, 2001

Computer purchasers
Females
Males
Home address
Business address
3 month
6 month
12 month
Lifestyle interest catego
Auctions
Beauty
Books
Cars
Computers
Computer software
Electronics
Entertainment
Financial services
Food cooking
Freebies
Gardening
Gifts
Health fitness
Home improvement
Horoscopes
Movies
Music