Privacy and Free Speech in the Political Landscape

For the Democracy Online Project

November 28, 2001

By Solveig Singleton[1] and James V. Delong[2]

Introduction

Private and anonymous communication has long played an important role in the American political tradition. It began with encrypted letters exchanged by American Revolutionaries such as Ben Franklin, John and Abigail Adams, and Thomas Jefferson. It continued with the Australian secret ballot, first used in New York in 1889 and adopted in 38 more states by 1896.[3] Perhaps the best example of the key role privacy has played in the American electoral politics comes from the case of *NAACP v. Alabama*, in which the Supreme Court upheld the constitutional right of the NAACP to operate in Alabama without complying with a state requirement that it turn over its membership lists.[4] The Court said that privacy was essential to "the freedom of individuals to associate for the collective advocacy of ideas," as guaranteed by the First Amendment. But privacy has

---

[1] Solveig Singleton is a lawyer and Senior Analyst with the Competitive Enterprise Institute's Project on Technology & Innovation.

[2] James V. DeLong is a lawyer and Senior Fellow with the Competitive Enterprise Institute's Project on Technology & Innovation.

[3] New York: Federal Elections Commission Website, http://www.fec.gov/pages/paper.htm.
Other states: Jonathan N. Katz & Brian Sala, "Electoral Reform and Legislative Structure: The Effects of the Australian Ballot Laws on House Committee Tenure," (April 1995), listed as forthcoming in *American Political Science Review*, http://wizard.ucr.edu/polmeth/working_papers95/katz95.html (visited Nov. 29, 2001).

[4] 377 U.S. 288 (1964).

also been upheld in less volatile situations, as in 1995, when the Supreme Court upheld the right of an Ohio woman to pass out anonymous leaflets concerning a local election.[5]

At the same time, the opposite principle -- the importance of the free movement of information -- has played an equally pivotal role in politics. This principle is also protected by the First Amendment, in this case the free speech clause, and in general it may be strongly opposed to what we think of as privacy. We recognize that speakers should be free to investigate and comment upon the lives of public figures, and the law raises the bar to defamation suits in such cases; a report must be not only erroneous but motivated by actual malice before it becomes actionable.[6] We allow solicitors of funds or political support to tramp from door to door, intruding on the homeowner's peace for the sake of furthering healthy public discourse. We allow handbills to be distributed despite the risk of littering, and private property to be treated as public for the sake of political speech.[7]

To generalize about these conflicting examples of privacy and the free movement of information, one may conclude that constitutional principles of privacy apply when the intruding information-seeker is the government, but free speech principles protect information-seeking on the part of the private sector, often, but not always, journalists.

This analysis addresses the issue of how new technology—particularly the Internet—will change the balance between confidentiality and open information in American politics. Two related issues are particularly important: (1) Is online profiling – the collection by a political website of information about its visitors – harmful or beneficial for the political process? (2) To what extent is it legitimate for political

[5] *McIntyre v. Ohio Elections Commission,* 514 U.S. 334 (1995).
[6] *New York Times v. Sullivan*, 376 U.S. 254 (1964).
[7] *Pruneyard Shopping Center v. Robbins*, 447 U.S. 74 (1980).

websites to engage in aggressive outreach, contacting people who have not asked to be placed on email lists?

The questions may have no long-term or permanent answer, because the nature of online profiling and online outreach used in online politicking are changing rapidly, with each new permutation potentially having a different cost-benefit analysis. But in the short run, the answer is clear: At present, the use of information gathered online in electioneering has the effect of helping political and grassroots groups to grow and find new supporters. Because using the Internet is much cheaper than using paper and television, profiling and outreach are probably most useful to "underdog" groups or new candidates operating on shoestring budgets. Thus these techniques have substantial potential for breaking the hammerlock on electoral processes now held by incumbent office holders and parties, and any effort to restrict them would be significantly anti-democratic.

This democratizing potential is augmented by the growth of citizen-operated websites. As early as May 2000, an estimated 6,700 home-grown websites were in operation, in anticipation of the November election.[8]

Uses of Online Information in Elections and Politicking

The use of the Internet in electioneering is growing rapidly. Candidates' and parties' web sites have become increasingly important as a means of sending out a political message not only in the United States but also in Canada and Australia. According to one Pew survey, one in five Americans reported going online for election

[8] Leslie Wayne, "On Web, Voters Reinvent Grass-Roots Activism," *New York Times*, May 21, 2000. Section 1.

information in 2000, up from 4 percent in 1996.[9] Candidates' sites and sites specializing in politics drew most visitors in 1996 as a source of political information, but in 2000 mainstream news sites became a much bigger draw, as many of them added special voter supplements, voting records, and records of campaign contributions.[10] The Pew survey also reports that experienced Internet users (45 percent of those online for at least three years) are more likely to use the web for political information than newcomers (17 percent of those who came online in the past six month).[11]

A political website faces the same basic problem as electronic merchants more generally. Clicks may come and clicks may go, but without some means of recording the clicks, the web site operator will be blind, dumb and deaf to the desires and nature of those entering and leaving their electronic shop. Thus "cookies" are deployed, helping the operator gain a sense of whether a given visitor has already registered there before, the flow of traffic to different parts of the web sites, exposure to banner ads, and so on. The types of cookies that appear on a political web site are generally of the type ordinarily used in commerce, with some being third-party cookies, some being permanent, others temporary, and so on.

Now we turn to the particular types of targeting electronic campaigns associated with political web sites. Most start-up sites begin with a short list of email or snail mail addresses of known supporters, family, and friends, perhaps someone's Christmas

[9] "What Americans Think: Election Information via the Internet," Vol. 74 Spectrum: The Journal of State Government (January 1, 2001).

[10] Leah Beth Ward, "Informative or Exhausting? Survey shows the Internet is Drawing Bigger Crowds, But They're Spending Less Time Online," *The Dallas Morning News*, February 19, 2001.

[11] Ibid.

card list. More email addresses are collected from those who register their names and email addresses online. In the recent governor's race in New Jersey, Bret Schundler asked supporters to contribute the names and email addresses of other known supporters amongst their family and friends.[12] Requests for fundraising, calls for volunteers, or campaign information may then be sent to the lists. The usual response rate to a direct mail fundraising campaign is two percent; targeting can bring it up to three to four percent. But using names of people who have themselves signed on at the web site yield response rates as high as ten percent.[13]

Simultaneously, the candidate, grassroots group, or issue groups will be busily collecting data offline, as well. The main sources of offline mailing lists include subscriber lists from relevant magazines or newspapers, lists belonging to other similar nonprofit organizations (usually traded rather than bought), sympathetic political parties (also usually traded), or PACs (usually offered as an in-kind contribution). For fundraising purposes, however, often only lists of actual donors to a similar cause are sought, if available, because the response rate to non-donor lists is so low.

Some political groups promise confidentiality of the names and addresses (collected online or offline), while others do not; one source estimated those promising confidentiality as opposed to those not at about 50/50.[14] In conservative circles, for example, the Christian Coalition traded information about supporters with other similar groups, while the Family Research Council, a group with a similar agenda, promised

[12] "Opinion – Capital Talk," *The Bergen Country Record*, Oct. 21, 2001.
[13] Author's Telephone Interview with J. Posey, Managers, Promotions and Production, Americans for Fair Taxation, September 19, 2001.
[14] Ibid.

confidentiality as an additional "selling point."[15] Organizations generally remove those who request removal from their lists (online or offline); there is no point in keeping them on. Campaigns run by one of our sources reported including an opportunity to opt out with every message sent.[16]

Some of the most valuable information used in election campaigns, however, does not come from the Internet. This offline information may be used by itself, or used to supplement a list of names and addresses collected online. For a campaign for political office, the most desirable information is party affiliation and voting record. A donor list, for example, might be built by identifying people who voted for a given political party in the last three elections. This information comes from voter registration lists provided by brokers like Aristotle.[17] Voter registration lists may include party affiliation or record which primary the voter voted in. The campaign assumes that if a voter has voted in the Democratic primary, he is likely to have voted Democrat in the main election. Aristotle can match voting history to email addresses to help target certain banner ads to certain visitors.

Another type of valuable information sought from offline sources is zip code. Traditionally, political campaigns would obtain lists of licensed drivers from the state and send messages to those in districts heavily affiliated with one political party or another. Now, Internet services can match email addresses collected online to physical names and addresses, including zip code.

[15] Author's Interview with L. Gilliam, former outreach campaign worker, September 14, 2001.
[16] Interview with J. Posey.
[17] http://www.aristotle.com/

Campaigns also seek to obtain information to target voters interested in specific issues. For example, some candidates have targeted fundraising materials to those with a special interest in gay or lesbian issues, abortion, or environmental issues. For this type of targeting, magazine and newsletter lists tend to be most useful. In the future cookies or other systems might be used much more extensively to build a picture of an online visitor's likes and dislikes or personality to play a larger role in targeting and tailoring the web site's outgoing communications to voters. Presently, however, most campaigns and grassroots groups appear to be mainly involved in the more primitive area of matching names and addresses collected online to a fairly limited offline data set.

How Might Targeted Email Change the Political Landscape?

The most obvious benefit of using targeted email and banner ads in campaigns for electoral candidates is that response rates to email campaigns are very high compared to traditional mail campaigns. And, the cost of sending out electronic messages like email or banner ads for a campaign online is much less than the cost of buying television, radio, or newspaper advertising or sending out direct mail. How is this new element in the equation likely to affect prominent features of the political landscape? Answering this requires taking a closer look at how campaigns have traditionally been conducted, and how they are funded.

The section above described how a start-up campaign or grassroots group would begin to collect lists, both offline and online. Subtract the online part, and the remainder describes how a start-up group would build a campaign—the slow build-up of any and all affordable lists, targeted by zip code or some proxy for political affiliation such as

subscribership to a conservative or left-leaning magazine, and voter registration information. In the absence of any money at all, though, any list that happened to be on hand would do. Americans for Tax Reform, for example, began with a list of some thousands of people who had bought Ginsu kitchen knives.

Incumbent political candidates, however, have unique opportunities to supplement their outreach activities. At the federal level, members of Congress may use their privilege to send "franked" mail. Franking privileges all members to use the mails free of charge for official business. In 1995, the average franking allowance for each member of Congress was $109,000, and this figure could be supplemented up to $25,000 from other sources.[18] The franking allowance would allow Congress to send nearly 1 million pieces of mail per year. Taxpayer money is also available to target that mail. In 1995, the House reportedly granted Aristotle a $250,000 development loan to move its databases onto CD-ROM. By the next summer fifty-six legislators had purchased the CD-ROMs for a total of $250,000.[19]

Because these privileges are not available to challengers, significantly fewer voters are reached by challengers than by incumbents. In 1994, 63 percent of voters got mail from incumbents, only 25 percent received mail from challengers.[20] A similar effect exists for other media. Congress has audio and film-preparation services free of charge to members for use in carrying out their official duties. Again, there is a significant gap between challengers and incumbents. In 1994, 33 percent of voters report hearing

[18] Eric O'Keefe and Aaron Steelman, "The End of Representation: How Congress Stifles Electoral Competition," Cato Institute Policy Analysis No. 279, August 20, 1997, p. 3.
[19] Ibid.
[20] Ibid.

incumbents on the radio, only 18 percent recalled hearing challengers.[21] Sixty-one reported seeing incumbents on television, 34 saw challengers.[22] Congressional offices have unlimited long-distance telephone services; in 1994, 14 percent of voters claimed they had talked with someone on the incumbent's staff, compared to 5 percent who had talked to someone working for the challenger.[23]

This incumbent advantage also extends to the use of the World Wide Web, as legislators in office have taxpayer-funded web sites. And, in 1996, Compuserve planned to offer free sites to incumbents and challengers alike. But the Federal Election Commission refused to allow it, on the ground that the offer of web sites to candidates for office would constitute an in-kind contribution.[24] Still, challengers can fund their own sites, can accept the in-kind contribution of a site, or simply use send out email without a site, or use a bulletin board online or a list-serv, as was done pre-Web. The alternatives here are substantially less expensive that starting a direct mail operation, doing telemarketing, or getting on radio or television. Direct mail costs a minimum of 21 cents per piece sent for printing and postage if bulk mail is used, 38 cents each for first class. Some sample costs for television, magazines, and the Internet, as of early 1999, are contained in the following table:

CPM Rates for Various Media [CPM is Cost per Thousand Impressions (number of times an ad gets seen) which is a typical cost measure for advertising rates] [25]

---

[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid. at 4.

[25] Source: Eric Rosenwald, McDonough School of Business, Georgetown University, *Branding Online*, Nov. 24, 1999, available at http://www.gsb.georgetown.edu/faculty/culnanm/EC/Briefings2/rosenwalde.html (Viewed Nov. 20, 2001).

Media	Vehicle	Cost	Reach	CPM
Television	30 second spot on "NBC Evening News"	$55,000	10M households	$5.5 per thousand households
Consumer Magazines	Full-page, four-color ad in Cosmopolitian	$86,155	2.5M paid readers	$34.46 per thousand paid readers
Website	Banner on InfoSeek	$10,000 per month	500,000 page views (guaranteed)	$20 per thousand page views
Online Service	Banner on one of CompuServe's major topic menu pages for one month	$10,000 per month	750,000 to 2M visits (estimated not guaranteed)	$13.33 per thousand visits (at 750,000 visits)

The possibility of targeting email over the Internet can be expected to continue to be a very important factor in helping challengers be more visible in their battles against incumbents. One challenger for state office facing an empty bank account at the start of his campaign used the in-kind contribution from a PAC of their donor's email list to send out his first fundraising piece by email. The single email campaign generated about $5000—at no cost to the candidate.[26]

The overall effect of the use of targeted email will be to lower the costs of entry into political campaigns for grassroots start-ups and new candidates. Of course, many of the incumbent's advantages will remain, as a natural part of holding public office is high visibility and the use of taxpayer funds. And a richer candidate will always be able to spend more on online efforts and targeting than a poorer candidate. But this is true of the entire online economy, and yet we have persistent evidence of relative "unknowns" being given their big break over the Internet, and the phenomenon shows no signs of slowing. In the case of campaigns and grassroots groups, even the very primitive targeting and "profiling" that goes on has been an important part of this phenomena.

[26] Interview notes on file with author, confidential by request of interviewee.

The Harms of Online Profiling

We now arrive at the question of the harms of online profiling. In terms of actual danger to visitors online, the collection of email names and addresses through is innocuous, as are trades of this information among sympathetic groups. The collection of donations online involves credit card numbers, and as such raises the possibility of unauthorized access to card numbers identical to those faced by electronic commerce merchants. Another risk is that "rogue" employees within an organization will use credit card numbers without authorization, the same risk that a credit card user faces in visiting a restaurant, gas station, or other such "real space" places. This is, however, not a risk that becomes any greater by the use of profiling or targeting of the email using information about someone's interests or voting record. Another type of harm that might arise from the increased use of the Web and email in politics is that it might provide opportunities for scams to set up political sites as "fronts." But this danger likewise exists regardless of whether the site engages in any kind of profiling. The possibility that registering one's name and email address at a political web site will invite some kind of criminal activity appear to be no larger than of participating in economic activity in general. Overall, the risk is negligible.

A second type of harm might be threatened. Suppose a rogue government were to seize the private lists and databases of political organizations so as to target members of groups it perceives as a threat. Fortunately, in the United States such ventures would be forestalled by the First Amendment, which historically has often protected the anonymity of such lists. Such seizures would also be regulated by the Fourth Amendment. In any event, there really is no alternative to bearing this type of risk. It would be simply

impossible for the political organizations to operate without some kind of lists of their supporters, targeted or otherwise.

A Separate Problem: The Perceived Harm of Profiling

Although profiling does not add much of significance to the risks of real harm that online users face, segments of the public may feel that it does. Some would argue that the perception that online profiling is harmful is itself a harm, as it could discourage participation in online politics. To be precise that effect would stem from the perception that profiling is harmful, rather than from the profiling itself.

Evidence that the public sees profiling as harmful comes largely from public opinion polls on privacy issues. To offer just one example, a recent study by the Pew Internet & American Life Project found that 86 percent think that companies should ask permission before sharing personal information with third parties; 54 percent viewed cookies as an invasion of privacy; and only 27 percent agreed that tracking consumers online helps improve content and service.[27] Few if any of these surveys have focused on online political profiling in particular, but address concerns about privacy in electronic commerce. But we expect these perceptions carry over to political profiling, particularly as political information is often perceived as sensitive. Several analyses have thus asserted that these sentiments about profiling would result or have resulted in less participation in electronic commerce; one might then predict there would be less participation in online politics as well.

The difficulty with this line of argument is that the expressions of "concern" expressed in public opinion polls are not consistent with the way people actually act online. As Chet Thompson of Prodigy noted, "Market surveys told Prodigy that people

[27]Brian Krebs, "People Want More Control Over Personal Info Online," *Newsbytes*, August 21, 2000.

wanted to do their grocery shopping by computer. They didn't."[28] So, people may say in response to leading questions from a pollster (and leading questions are a substantial problem in almost all the polls)[29] that they are substantially or very or somewhat concerned about privacy.

But in fact these concerns are not significant enough to stop most people from going online. For example, some surveys show very high levels of "concern" or "discomfort" with giving out credit card numbers and Social Security Numbers.[30] But 75 percent of Internet users reporting having actually provided credit card numbers online, and 52 percent have provided their Social Security Number online.[31] Fifty-five percent of Americans bought something online during the 2000 holiday season, up from only 20 percent in 1998. Credit card transactions online are growing by leaps and bounds; there were 4.9 million such transactions online in 1997, 9.3 million in 1998, and 19.2 million in just the 3rd quarter of 1999.[32] And Web site operators report low attention to privacy policies. The former Chief Privacy Officer of Excite@Home, for example, told a March 13, 2001, Federal Trade Commission workshop that, on the day after that company was

[28] Peter K. Pitsch, *The Innovation Age: A New Perspective on the Telecom Revolution* (Washington, D.C.: The Hudson Institute and the Progress and Freedom Foundation 1996): 48.
[2929] Jim Harper and Solveig Singleton, "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," Competitive Enterprise Institute Monograph, June, 2001; *See also*, Michael A. Turner and Robin Varghese, "Making Sense of the Privacy Debate: A Comparative Analysis of Leading Consumer Privacy Surveys," DMA Information Services Executive, 2001.
[30]The Arthur Andersen study found only 2 percent comfortable with giving out their Social Security Number online, and only 8 percent comfortable with giving out credit card number. The AT&T study reports 1 percent of consumers comfortable with giving out Social Security Numbers, and 3 percent comfortable with giving out credit card numbers.
[31] Harris Interactive/Privacy Leadership Initiative Survey, December 2000, p. 15.
[32] Cyber Dialogue, "Best Practices" at 2.

featured in a *60 Minutes* segment about Internet privacy, only 100 out of 20 million unique visitors accessed that company's privacy pages.[33]

The least manipulative and probably most accurate form of consumer survey is an unprompted survey, in which people are asked to list the issues of concern to them *without being prompted or given a list of possible responses.* This type of survey is often used to identify election issues because candidates need to know what will motivate votes, not just what voters will say to a pollster. In recent such surveys, privacy simply does not appear among top concerns.[34]

In short, predictions that concerns about privacy would dry up Internet activity appear to be vastly exaggerated.

The Potential Regulation of Online Profiling

In analyzing possible mechanisms for controlling profiling, it is important to start with the understanding that a website must have the cooperation of the person logging on before it can obtain information about that person. Programs that monitor website traffic capture only the domain whence a hit originates – they do not get the individual email address or any other personal data. Before information is collected by the site, it must be provided by the individual.

However, there is a caveat to this general proposition. So much information is available on the Internet now that collection of a small amount of data, such as an email

[33]Workshop on "The Information Marketplace: Merging and Exchanging Consumer Data," Federal Trade Commission, March 13, 2001 (comments of Ted Wham) <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm>.
[34] See, e.g. Peter Raducha, "Preliminary Results of a Nationwide Survey of Youth," Global Youth Action Network, July 2000; Frank Newport, "Economy, Education, Health, Crime and Morality Most on Americans' Minds This Election Year," *Gallup News Service*, June 22, 2000.

address or a name and city, provides a lever to collect much more. For example, running "James V. DeLong" through the search engine Google produced over 900 discrete hits. Most were to various writings, but the author's address, place of employment, and telephone number were also there. If proprietary databases were accessed, his credit history and other information would be available (although access to credit reports is restricted by the Fair Credit Reporting Act).

As a recent article points out:

> Map Applications . . . can link more than 40 layers of personal data to a voter's name and address, and then make sense of it all. The information includes voters' ages along with their children's ages, the value of their homes, whether they have bank cards, and their ethnicity. Much of the data resold by Map Applications originated with credit bureau giant Trans Union . . . .[35]

One item of information that would *not* be legally available would be the individual's history of contributions to federal election campaigns. The Federal Election Campaign Act provides:

> Information copied from such reports or statements [filed with the FEC] may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee. [36]

To enforce this provision, the recipient campaign committee is allowed to seed its reports with phony names so that any list drawn from the reports will contain these telltales of their derivation. This may prevent the use of the reports for the development of massive lists, but one is entitled to be skeptical that political and charitable solicitors always resist the temptation to check on the political contribution history of a potential contributor, given the easy availability of the data. Morever, the recipient compaign itself is not prohibited from selling, renting, or trading its donor list with others. As one

[35] "Campaign Finance: Campaigns' Profiling Stirs Privacy Worries," *George*, October 2000.
[36] 2 U.S.C. 438(a) (4).

election law expert notes: "[B]y using any number of existing Web sites, it is easy to plug in an individual's name and access a list of his or her political donations of more than $200. Thus, employers, business colleagues, customers, clients and neighbors now have a window into your political beliefs." [37]

To the extent this presents a privacy problem, however, the problem is created by the government's campaign finance reform laws, not by the Internet. The laws represent a judgment that individuals' political contributions should be made public because the public's need for information about political donations outweighs the individuals' right of privacy.

The questions of privacy that arise in the context of political websites are similar to those presented by commercial sites: What uses may be made of the information supplied by the individual? What about information that is collected based on the information furnished by the individual? What requirements should the website fulfill before using the information?

Uses to which information can be put are frequently categorized into the categories of primary, secondary, and tertiary.

Primary uses encompass the purpose for which the individual is furnishing the information. For example, if someone buys a book from Amazon, then he must give his address so that the book can be delivered. He provides a credit card number so that sale can be consummated.

Secondary uses encompass other uses of the information by the site to which the information is supplied. Information is often used to develop a continuing relationship

[37] William Farah, Lawmakers Should Preserve the Right To Political Privacay on Net," *BRW Roll Call*, August 9, 2001.

with the individual, sending him notices about new products and in other ways soliciting further business.

Tertiary uses occur when the site to which the information was furnished passes it on to another party. In the context of political groups, for example, organizations might want to trade information. Someone who contributes to the Sierra Club may be regarded as a good prospect for the Environmental Defense Fund, and vice versa, and the groups might agree to trade lists. This can extend to candidates who take positions favored by the organization. A candidate might very much like to get her hands on the Sierra Club's email list--and mailing list, for that matter, if she has a record of favoring more intensive regulation of the environment.

A category that does not fit easily into this taxonomy concerns the generalized use of information. That is, information about an individual is integrated into a broader data base about consumers or contributors, but the individual remains anonymous. These data bases can be used either by the organization operating the website or can be made available, through sale or otherwise, to other organizations, such as market researchers or political scientists.

There are two major ways in which the collection and use of information by political websites can be controlled – voluntary actions by websites in pursuit of their self interest, and government regulation. Whichever mechanism is used, the same three basic tools are used: Notice; Opt-Out; and Opt-In.

Political websites, like commercial websites, have strong incentives to treat their clients carefully. A potential customer who feels that his privacy has been violated quickly becomes a non-customer. Similar, a potential supporter who is offended

becomes an ex-supporter. In fact, the political site has an even greater incentive to avoid giving offense. The worst that an offended customer can do is refuse to buy. In a political context, someone who is offended can become an activist on the other side. Since a basic rule of politics is to avoid energizing the opposition's base, all sites walk carefully.

The most basic tool for protecting privacy is Notice. The individual is informed that the website is collecting information, and know that proceeding with the transaction will allow this. Notice as to primary uses seems superfluous; obviously, the address must be furnished before the book is shipped, and consent for this use can be assumed from the structure of the transaction. Similarly, some information must be supplied by the individual logging on to a political website, if he wants to be sent information or contacted again, and it can be presumed that this is known.

Notice about secondary and tertiary information can be important, however, for focusing the individual's attention on the broader possible secondary and tertiary uses of the information.

Notice is sometimes branded inadequate because it presents the individual with a "take it or leave it" situation, but in fact it is a valid method of protection. Presented with the choice, the individual decides that he values the transaction sufficiently to consent to the use of the information. He is better off, by his own lights, because the website is induced to provide services for which receiving the information may be compensation.[38]

Realistically, however, few political websites are likely to insist on obtaining information from an individual in exchange for supplying information to him or her. If

[38] Solveig Singleton, "A Market Approach to Consent," in Advisory Committee of the Congressional Internet Caucus, *Privacy Briefing Book 2001*, available at http://www.netcaucus.org/books/privacy2001/ (visited November 20, 2001).

someone is curious about the campaign, in the case of a candidate, or about the issue, in the case of an advocacy group, then it is in the interest of the web site operators to push information out to him or her in the hopes of making a convert. Insisting on information in exchange is a short-sighted strategy.

The next level of protection is Opt-Out. In this model, the individual is informed that information provided will be put to secondary or tertiary uses unless the individual specifically requests that this not be done. The default, if the individual reacts passively, is that the information is used. An alternative, more stringent approach is Opt-In. In this mode, the individual must specifically consent to the use of the information. A passive response means that the information is *not* used for secondary or tertiary purposes.

The lines between pure notice, opt out, and opt in are not bright. For example, to exercise an opt out might require the individual to click through several screens to find the right button in a long paragraph about privacy policy. And the difference between op out or opt in can be as simple as the difference between putting a check in a box as a default or leaving it blank. For example, a website might say: "If you want us to share your information with trusted partners who will give you great deals, leave a check in the following box:" If the box is already checked, so that the individual must remove it, then the system is classified as an opt out. If the box is blank, so the individual must add a check, then the system is opt in.

In addition, of course, and under either system, disclosures about the uses to which the information will be put can vary widely. In the commercial world, very few websites provide much specificity, usually limiting themselves to vague comments about additional products or special offers.

Both commercial firms and advocacy groups are concerned about creating a backlash of ill will from those who log on. As noted earlier, many promise not to release individual data to anyone else, fearing that any other policy will discourage possible supporters.

Two aspects of the issue are seldom discussed. Virtually no website mentions the possibility that it can take the barebones information of a person's email or name and city and turn it into a more complete profile, perhaps using Google. Thus people are often not fully aware just how much information might ultimately be obtained about them using their initial entry.

Websites vary in stating their policy on collecting and sharing aggregated information. Some make clear to customers that this is being done. Others take the view that the customer actually has no particular privacy interest in not being part of a database, that customers as a whole can benefit greatly from the creation of such databases, that explaining the economic benefits is too difficult and chancy, and thus that disclosure is not necessary.

Some campaigns or advocacy groups reach out aggressively. During the 2000 campaign the National Rifle Association bought lists of pickup truck owners, holders of hunting licenses, weapons carry permits, gun show exhibitors and outdoor magazine subscribers. The National Abortion and Reproductive Rights Action League constructed lists of two million Republican and Independent women to reach, after constructing a

demographic portrait of its own supporters and then seeking women who "visit the same Web sites, listen to the same radio stations, or read the same newspapers."[39]

Activities directed at such potential supporters need not be conducted over the Internet, of course, and merging lists is a practice that long predates the Internet and even the computer. But the rise of the Internet has increased the amount of information available, and email is an effective way to respond to the new information.

When the Internet is used aggressively, it runs directly into the current controversy over Internet spam.

Whether a message is spam depends to some extent on the mind of the beholder. Almost everyone agrees that the term should include unsolicited commercial email that is sent without a return address and that includes no provision for removing oneself from the list. However, some who call themselves "anti-spam" go much further. The Mail Abuse Prevention System (MAPS), a private group that blacklists IP addresses when MAPS clients turn them in for spamming, insists that no one be put on an email list unless they opt in twice – first by clicking to go to a website and then by accepting the list once they get there.[40]

Even in the commercial context, people are ambivalent about the correct standard. Receiving multitudinous emails asking if one wants to become a Reverend, which seems to be the latest spam *de jour*, soon becomes tiresome. On the other hand, advertising does indeed provide useful information, and it is difficult to draw the line. Besides, a large amount of spam, which can be quickly deleted at a time of one's choosing, is less

[39] John Mintz & Robert O'Harrow, Jr., "Software Digs Deep into Lives of Voters; Campaigns' Profiling Stirs Privacy Worries," *Washington Post*, Oct. 10, 2001, http://www.loper.org/~george/archives/2000/Oct/90.html (visited Nov. 19, 2001).
[40] Brenda Sandburg, "The Legal Challenge of Canning Spam," *The Recorder*, Oct. 23, 2001.

intrusive than one telemarketing call during dinner, and blipping an email takes less time than opening an unsolicited letter, so it is sometimes difficult to understand the intensity of outrage generated by the spam issue. The real underlying problem may be not the messages are unsolicited but that so many of them are obscene, fraudulent, or both. If these categories were eliminated, then the volume would be considerably lessened.

Some states have passed anti-spam laws and Congress is constantly considering legislation. But there is no agreement as to the desirable features or on avoiding blockage of beneficial communications.

The fundamental concept of spam is especially tricky in the political context. A die-hard Democrat might regard any unsolicited message from a Republican organization as spam, and vice versa. But it is hard to imagine that any law prohibiting unsolicited political or issue-oriented emails would be constitutional. Protecting people against new ideas is not one of the goals of our democracy. Indeed, as mentioned at the beginning of this paper , the courts have consistently allowed "real space" political activists to intrude upon what private property.

On balance, we should be very slow to adopt any methods of top down regulatory control over political sites and their use of information. Experience in the context of commercial enterprises establishes two important points. The first is that writing regulations that would be effective without imposing unintended consequences is very difficult. A major reason privacy legislation has not gone forward is that the issues are difficult, and the judgments involved do not lend themselves to government fiats.

The second lesson from the commercial context is that business enterprises are wary of offending the public, and bend over backward to avoid anything that could be

construed as an invasion of privacy. Many have adopted an opt-in policy, despite its greater stringency, and when an opt out policy is invoked the choice is usually obvious and easy to exercise. Notice provisions and privacy policies are virtually universal on large sites, and most guarantee not to make individually identifiable information available.

As noted earlier, consumers seem more concerned about privacy when they are asked about it in the abstract than when they are making concrete choices –few read the policy even when prompted. Given this reality, the market seems to be providing an appropriate level of protection.

The problems of effective regulation are compounded when political activity is involved. The Internet has the potential to be a substantial equalizer between incumbents and challengers, or between established ideas and advocacy groups and upstarts. Regulations would be written by incumbents for the benefit of existing groups. It is safe to say that any effort to regulate Internet political activities in would introduce still more sclerosis into the system. This has been the experience with campaign finance reform laws, where the protection of the status quo has been elevated to an art form, and the same incentives would govern any efforts to control Internet politicking.[41]

Profiling and the First Amendment

A close corollary of the question as to whether profiling does more harm than good to political activity online is whether gains would be realized from restricting profiling (online or otherwise) in some way. The answer is that restricting profiling would pose a significant threat to rights of speech and association protected by the first

[41] James V. DeLong, "Free Money," *Reason*, Aug./Sept. 2000, http://reason.com/0008/fe.jd.free.shtml.

amendment. That the maintenance of membership lists held by political association is already well established in *NAACP v. Alabama*. But imagine if, instead of trying to obtain the NAACP's membership list itself, the state chose to regulate instead the NAACP's use of its list, its attempts to contact more African-Americans to join the organization, its attempts to expand the list. The state might even put forward a noble motive, that political information is especially sensitive and that private actors or organizations might abuse lists of those with a strong interest in civil liberties issues and voting rights. This regulation would, however, be as quick a route to shutting down the NAACP as forcing disclosure of the list would be. To deny organizations—especially political organizations—the freedom to innovate and use new technologies to bring their message to interested members of the public without mowing through yards of red tape, would strike at the very heart of what the first amendment protects.

Consistent with this, it is noteworthy that Europe's Data Protection Directive—broad regulation of the use of consumer information even by the private sector—exempts synagogues, trade unions, churches, and other nonprofits that keep even "sensitive" information about their members. It is hard to imagine how these groups would function if they did not.[42]

Let us explore some of the elements of profiling as protected speech in more detail. Let us begin with the basic element of online profiling—a list of email addresses and names. Someone's name and address is a fact about the someone, conveying information as to their physical or (in the case of email) virtual whereabouts. Matching name and address to voting records or to zip code adds more information. Aside from the

[42] Solveig Singleton, " Privacy and Human Rights: Comparing the United States to Europe," *printed in The Future of Financial Privacy: Private Choices Versus Political Rules* 188 (Washington, D.C: Competitive Enterprise Institute 2001).

occasional error, for the most part this information is truthful information—not false speech like defamation. Trade or sale of lists is as much an exchange of truthful speech as the sale of a book or the distribution of a pamphlet. Regulation of some trades explicitly for funding might potentially be viewed as commercial speech (thus would still be protected, just under a lower standard) but this is much less likely in the case of trades by nonprofits or political campaigns, especially in light of precedents that declare that campaign donations are themselves a sort of political speech.

There has been, of course, little precedent in this area, as this routine trade has continued for the most part free of regulation (with the exception of credit reports), and what regulation there is has not often been challenged. There is, however, a substantial body of precedent supporting the idea that transfers of information derived from public records are protected by the First Amendment. In *Cox Broadcasting v. Cohn*,[43] the United States Supreme Court overruled the Georgia Supreme Sourt's decision to uphold a plaintiff's suit under a law that made it a misdemeanor to publicly disseminate the name of a rape victim. The Court said, "if there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information. . . . Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it."[44] Following this case, courts have consistently held that information gleaned from public records may not be suppressed consistent with the First Amendment.[45]

---

[43] 420 U.S. 469 (1975).
[44] Ibid. at 496.
[45] See Legi-Tech, Inc. v. Keiper, 766 F.2d 728, 730 (2d Cir. 1985); Federal Election Comm'n v. Political Contributions Data, Inc., 943 F.2d 190, 196 (2nd Cir. 1991); U.D. Registry v. State, 34 Cal. 4th 107; 40 Cal. Rptr. 2d 228 (Cal., 1995).

A constitutional loophole of sorts apparently remains in this case law. The *Cox* case explains that the state could choose at the outset simply not to make the matter a part of the public record. A state might decide, for example, that voter registration lists would in the future be closed and not publicly available at all. This would take the privacy-enhancing action out of the reach of current precedents. But it would not resolve the basic problem—withdrawing this information from the reach of political parties would cripple the political process, unless the same information were available from other sources.

The question remains, how much would a system of regulation burden such speech. A notice requirement might not be unduly burdensome—but even a simply notice requirement can quickly turn into densely problematic legalese and significant liability risks. Opt-out is less burdensome than opt-in, but again, if the law is executed badly so to create massive liability risks, a substantial chill on organization's outreach efforts might be expected. This would have a particular impact on smaller groups insufficiently funded to afford expensive legal counsel. Opt-in is the least likely of these options to pass scrutiny. It is not necessary to prevent any real harm to the public and would in effect shut down many types of outreach activity.

The danger that privacy regulation would be badly executed in such a way as to harm political activity is a very real one. In Britain, a neo-Nazi sympathizer used the pretext of demanding "access" to his files under the data protection law to harass a Jewish organization that kept files on Nazi war criminals. In Sweden, a law was passed making it illegal to publish personally identifiable information on the Internet. The prosecutor was embarrassed to discover that a literal reading of the law meant a human-

rights group could no longer legally have a web site with the heading "Pinochet is a murderer." The prosecutor tried to save the situation by explaining that minor violations of the law would not be prosecuted. But this resort to prosecutorial discretion has not saved animal-rights groups and consumer activists from liability under the privacy law.

If targeting were substantially chilled or regulation out of existence, it would have the effect of forcing organization to return to a "broadcast" model of outreach. This entails sending as much information to as many people as possible, in the hope that some of them are interested. To force to speak to all means that some organizations will speak to none, if those interested in their cause are only thinly dispersed through the populace, they will simply not be able to reach a enough people to maintain the viability of their organization. The more a group is in the minority, the more it will be harmed.

Conclusion

On balance, the ancient prime directive of medicine applies: First of all, be sure that you do no harm. While privacy concerns exist, online profiling as it exists today can also make communication of information between politically active individuals much more efficient. The representatives of one set of interests will find that the costs of contacting others who share their interests can decrease substantially, as targeted communications are sent only to the most likely prospects. This will be of particular benefit to groups representing narrow minorities, or operating on a limited budgets. Online activity holds out great promise of leveling the political playing field in exciting and profoundly pro-democratic ways.

Given these circumstances, we should be exceedingly wary of proposals to regulate and restrict, particularly when those proposals are directed at harms that are hypothetical rather than actual. Granted, the potential exists for intrusions into people's justified expectations of privacy, and some such intrusions will undoubtedly occur. Nonetheless, premature restrictions could stifle a promising and productive developments that will improve the functioning of American democracy.

About The Competitive Enterprise Institute

The Competitive Enterprise Institute is a public policy organization dedicated to the principles of free enterprise and limited government. Founded in 1984, CEI promotes pro-market policies and the institutions of liberty through analysis, education, coalition building, advocacy, and litigation. CEI is nationally recognized as a leading voice on a broad range of regulatory issues ranging from environmental laws to antitrust policy to regulatory risk. CEI is a nonprofit, tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code.