

HEINONLINE

Citation: 1 Controlling the Assault of Non-Solicited Pornography
Marketing CAN-SPAM Act of 2003 A Legislative History
H. Manz ed. 8238 2004

Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Mon Apr 22 11:07:08 2013

- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at <http://heinonline.org/HOL/License>
- The search text of this PDF is generated from uncorrected OCR text.

Census. Even the use of letters, diaries, and other first-person recordings of slave simply do not exist because slaves could not legally learn to read or write.

We may think after 1865, African Americans could then begin to use traditional genealogical records like voter registrations and school records. However, African Americans did not immediately begin to participate in many of the privileges of citizenship, including voting and attending school. Discrimination meant the prevention of African American sitting on juries or owning businesses. Segregation meant segregated neighborhoods, schools, churches, clubs, and fraternal organizations. Therefore, many of the records were also segregated. For example, some telephone directories in South Carolina did not include African Americans in the regular alphabetical listing, but at the end of the book. An African American must maneuver these distinctive nuances in order to conduct proper genealogical research. In my own State of Louisiana, descendants of the 9th Cavalry Regiment and the 25th Infantry Regiment, known as the Buffalo Soldiers, would have to know to look in the index of the United States Colored Troops and not the index of the State Military Regiments.

Abraham Lincoln said, "a man who cares nothing about his past can care little about his future." In 1965, Alex Haley stumbled upon the names of his maternal great-grandparents while going through post-Civil War records at the National Archives here in Washington, D.C. This discovery led to an 11-year journey that resulted in the milestone of literary history, *Roots*. By providing \$5 million for the National Historical Publications and Records Commission to establish and maintain a national database, the SEARCH Act proposes to significantly reduce the time and painstaking efforts of those African Americans who truly care about their American past, and care enough to contribute to the American future. This bill also seeks to authorize \$5 million for States, colleges, and universities to preserve, catalogue, and index records locally.

In a democracy, records matter. The mission of NARA is to ensure that anyone can have access to the records that matter to them. The SEARCH Act of 2003 helps to fulfill that mission by helping African Americans to navigate the genealogical process, given the circumstances unique to the African American experience. No longer should any American have to wait to find out about information leading to freedom.

I hope my colleagues will join me in celebrating Juneteenth this year by passing this measure, and I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1292

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Servitude and Emancipation Archival Research Clearinghouse Act of 2003" or the "SEARCH Act of 2003".

SEC. 2. ESTABLISHMENT OF DATABASE.

(a) IN GENERAL.—The Archivist of the United States shall establish, as a part of the National Archives, a national database consisting of historic records of servitude and emancipation in the United States to assist African Americans in researching their genealogy.

(b) MAINTENANCE.—The database established by this Act shall be maintained by the National Historical Publications and Records Commission.

SEC. 3. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated—

- (1) \$5,000,000 to establish the national database authorized by this Act; and
- (2) \$5,000,000 to provide grants to States and colleges and universities to preserve local records of servitude and emancipation.

By Mr. HATCH (for himself, Mr. LEAHY, Mr. SCHUMER, Mr. GRASSLEY, Mrs. FEINSTEIN, Mr. DEWINE, and Mr. EDWARDS):

S. 1293. A bill to criminalize the sending of predatory and abusive e-mail; to the Committee on the Judiciary.

Mr. HATCH. Mr. President, I rise to introduce, with Senators LEAHY, SCHUMER, GRASSLEY, FEINSTEIN, DEWINE, and EDWARDS, the Criminal Spam Act of 2003. This legislation, which enjoys bipartisan support, targets the most egregious types of spammers—those who hijack computer systems and those who use other fraudulent means to send unsolicited commercial electronic mail.

Over the course of the past several years, the amount of unsolicited commercial email, or spam, has grown at an exponential rate. During a recent Senate hearing before the Committee on Commerce, Science and Transportation, Brightmail Inc., a provider of spam filtering software that serves six of the ten largest U.S. Internet service providers, estimated that in April 2003, 46 percent of all email traffic was spam. This figure represented a nearly five fold increase in spam in merely 18 months. At the same hearing, America Online testified that on any given day, it blocks approximately 2.3 billion spam messages.

This tremendous growth rate is due in large part to sophisticated spammers who use abusive tactics to send millions of email messages quickly, at an extremely low cost. By using deceptive methods, these spammers conceal their identities, evade Internet service provider filters, and exploit the Internet by advertising and promoting pornographic web sites, illegally pirated software, questionable health products, pyramid schemes and other "get rich quick" or "make money fast" scams. The extraordinary volume of spam generated by their schemes imposes significant costs on Internet

users, threatens to disrupt Internet services, and undermines the public's confidence in online commerce.

A recent study conducted by the Federal Trade Commission demonstrates the alarming frequency with which spammers are using the Internet to conceal their true identities and the electronic paths of their messages. This study found that 40 percent of email messages contain indicia of falsity in the body of the message; approximately 33 percent contain indicia of falsity in the "from" lines of the spam; 22 percent contain indicia of falsity in the "subject" line; and some 66 percent contain at least one form of deception.

The Criminal Spam Act of 2003 targets fraudulent and deceptive spam by enhancing the ability of federal law enforcement authorities to prosecute and punish the most egregious wrongdoers. Specifically, the Act makes it a crime to hack into a computer, or to use a computer system that the owner has made available for other purposes, as a conduit for bulk commercial email. The Act also prohibits sending bulk commercial email that conceals the true source, destination, routing or authentication information of the email, or is generated from multiple email accounts or domain names that falsify the identity of the actual registrant.

The Act subjects violators to stiff criminal penalties of up to 5 years' imprisonment where the offense is committed in furtherance of any felony, or where the defendant has previously been convicted of a similar Federal or state offense, and up to 3 years' imprisonment where other aggravating factors exist. It also contains criminal forfeiture provisions and directs the Sentencing Commission to consider enhancements for offenders who obtain email addresses through illegal means, such as harvesting.

The strong deterrent effect of the legislation is further enhanced by civil enforcement provisions that authorize the Department of Justice and aggrieved Internet service providers to bring suit for violations of the Act. In appropriate cases, courts may grant injunctive relief, impose civil fines, and award damages of up to \$25,000 per day of violation, or between \$2 and \$8 per email intiated in violation of the Act.

Recognizing that spammers can send their fraudulent and deceptive messages from any location in the world, the Act directs the Department of Justice and the Department of State to work through international fora to gain the cooperation of other countries in investigating and prosecuting spammers worldwide and to report to Congress about their efforts and any recommendations for addressing international predatory spam.

The Criminal Spam Act represents an important legislative step toward curbing predatory and abusive commercial email. However, broader legislative measures, coupled with technological

solutions, are also needed. Any effective solution to the spam problem requires cooperative efforts between the government and the private sector, as well as the assistance of our international partners.

Recent years have witnessed extraordinary technological advances. These innovations, and electronic communications in particular, have significantly increased the efficiencies, productivity and conveniences of our modern world. The abusive practices of fraudulent spammers threaten to choke the lifeblood of the electronic age. This is a problem that warrants swift but deliberative legislative action. I am committed to working with my colleagues in both Houses to address the spam problem on all fronts.

I ask unanimous consent that a section-by-section analysis be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

SECTION-BY-SECTION ANALYSIS

SEC. 1. SHORT TITLE

This bill may be cited as the "Criminal Spam Act of 2003".

SEC. 2. PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL EMAIL

This section targets the four principal techniques that spammers use to evade filtering software and hide their trails. It creates a new federal crime that prohibits hacking into a computer, or using a computer system that the owner has made available for other purposes, to send bulk commercial email. It also prohibits sending bulk commercial email that either conceals the true source, destination, routing and authentication information of the email, or is generated from multiple email accounts or domain names that falsify the identity of the actual registrant. Penalties range from up to 5 years' imprisonment where the offense was committed in furtherance of any felony, or where the defendant was previously convicted of a similar federal or state offense, and up to 3 years' imprisonment where other aggravating factors exist. The U.S. Sentencing Commission is directed to consider sentencing enhancements for offenders who obtained email addresses through improper means, such as harvesting.

In addition, this section provides for civil enforcement by the Department of Justice and aggrieved Internet service providers against spammers who engage in the conduct described above. In appropriate cases, courts may grant injunctive relief, impose civil penalties, and award damages.

SEC. 3. REPORT AND SENSE OF CONGRESS REGARDING INTERNATIONAL SPAM

Recognizing that an effective solution to the spam problem requires the cooperation and assistance of our international partners, this section asks the Administration to work through international fora to gain the cooperation of other countries in investigating and prosecuting spammers worldwide, and to report to Congress about its efforts.

Mr. LEAHY. Mr. President, I am pleased to be introducing, with Senators HATCH, SCHUMER, GRASSLEY, FEINSTEIN, DEWINE, and EDWARDS, the Criminal Spam Act of 2003. This bill is designed to counter the most objectionable forms of email marketing. In an effort to clear electronic channels for legitimate communications, the

bill targets those spammers who deceive Internet Service Providers, "ISPs", and email recipients into thinking that messages come from someone other than a spammer—a ploy many spammers use to increase the likelihood that their unwanted ads will evade filtering software and be opened.

Without a doubt, spam is a serious problem today, one that is threatening to undermine the vast potential of the Internet to foster the free exchange of information and commerce. Businesses and individuals currently wade through tremendous amounts of spam in order to access email that is of relevance to them—and this is after ISPs, businesses, and individuals have spent time and money blocking a large percentage of spam from reaching its intended recipients.

Email users are having the online equivalent of the experience of the woman in the Monty Python skit, who seeks to order a spam-free breakfast at a restaurant. Try as she might, she cannot get the waitress to bring her the meal she desires. Every dish in the restaurant comes with Spam; it's just a matter of how much. There's "egg, bacon and Spam"; "egg, bacon, sausage and Spam"; "Spam, bacon, sausage and Spam"; "Spam, egg, Spam, Spam, bacon and Spam"; "Spam, sausage, Spam, Spam, Spam, bacon, Spam, tomato and Spam"; and so on. Exasperated, the woman finally cries out: "I don't like Spam! . . . I don't want ANY Spam!"

Individuals and businesses are reacting similarly to electronic spam. A Harris poll taken late last year found that 80 percent of respondents view spam as "very annoying," and fully 74 percent of respondents favor making mass spamming illegal. They are fed up.

ISPs are doing their best to shield customers from spam, blocking billions of spam each day, but the spammers are winning the battle. Millions of unwanted, unsolicited commercial emails are received by American businesses and individuals each day, despite their own, additional filtering efforts. A recent study by Ferris Research estimates that spam costs U.S. businesses \$8.9 billion annually as a result of lost productivity and the need to purchase more powerful servers and additional bandwidth; to configure and run spam filters; and to provide help-desk support for spam recipients. The costs of spam are significant to individuals as well, including time spent identifying and deleting spam, inadvertently opening spam, installing and maintaining anti-spam filters, tracking down legitimate messages mistakenly deleted by spam filters, and paying for the ISPs' blocking efforts.

And there are other less prominent but equally important costs of spam. It may introduce viruses, worms, and Trojan Horses into personal and business computer systems, including those that support our national infrastructure. It is also fertile ground for decep-

tive trade practices. The FTC recently estimated that 96 percent of the spam involving investment and business opportunities, and nearly half of the spam advertising health services and products, and travel and leisure, contains false or misleading information.

This rampant deception has the potential to undermine Americans' trust of valid information on the Internet. Indeed, it has already caused some Americans to refrain from using the Internet to the extent that they otherwise would. For example, some have chosen not to participate in public discussion forums, and are hesitant to provide their addresses in legitimate business transactions, for fear that their email addresses will be harvested for junk email lists. And they are right to be concerned. The FTC found spam arriving at its computer system just nine minutes after posting an email address in an online chat room.

At a recent FTC forum on spam, experts agreed that the issue is ripe for Federal action. Some 30 States now have anti-spam laws, but the nature of email makes it difficult to discern where any given piece of spam originated, and, thus, what State has jurisdiction and what State law applies. This may explain why spammers continue to flout State laws. For example, several States require that spam begin the subject line with "ADV," but the FTC has found that only 2 percent of spam contains this label.

Technology will undoubtedly play a key role in fighting spam. However, a technological solution to the problem is not predicted in the foreseeable future. In addition, given the adroitness with which spammers adapt to anti-spam technologies, the development and implementation of technological fixes to spam entail constant vigilance and substantial financial investment. This raises the question: Why should individuals and businesses be forced to invest large amounts of time and money in buying, installing, and maintaining generation after generation of anti-spam technologies?

I have often said that the government should regulate the Internet only when absolutely necessary. Unfortunately, spammers have caused this to be one of those times. Congress needs to address the spam problem quickly and prudently, and the Criminal Spam Act, by targeting the most injurious types of spam, is a good start.

The bill that Senator HATCH and I introduce today would prohibit the four principal techniques that spammers use to evade filtering software and hide their trails.

First, our bill would prohibit hacking into another person's computer system and sending bulk spam from or through that system. This would criminalize the common spammer technique of obtaining access to other people's email accounts on an ISP's email network, whether by password theft or by inserting a "Trojan horse" program—that is, a program that unsuspecting users

download onto their computers and that then takes control of those computers—to send bulk spam.

Second, the bill would prohibit using a computer system that the owner makes available for other purposes as a conduit for bulk spam, with the intent of deceiving recipients as to the spam's origins. This prohibition would criminalize another common spammer technique—the abuse of third parties' "open" servers, such as email servers that have the capability to relay mail, or Web proxy servers that have the ability to generate "form" mail. Spammers commandeer these servers to send bulk commercial email without the server owner's knowledge, either by "relaying" their email through an "open" email server, or by abusing an "open" Web proxy server's capability to generate form emails as a means to originate spam, thereby exceeding the owner's authorization for use of that email or Web server. In some instances the hijacked servers are even completely shut down as a result of tens of thousands of undeliverable messages generated from the spammer's email list.

The bill's third prohibition targets another way that outlaw spammers evade ISP filters: falsifying the "header information" that accompanies every email, and sending bulk spam containing that fake header information. More specifically, the bill prohibits forging information regarding the origin of the email message, the route through which the message attempted to penetrate the ISP filters, and information authenticating the user as a "trusted sender" who abides by appropriate consumer protection rules. The last type of forgery will be particularly important in the future, as ISPs and legitimate marketers develop "white list" rules whereby emailers who abide by self-regulatory codes of good practices will be allowed to send email to users without being subject to anti-spamming filters. There is currently substantial interest among marketers and email service providers in "white list" technology solutions to spam. However, such "white list" systems would be useless if outlaw spammers are allowed to counterfeit the authentication mechanisms used by legitimate emailers.

Fourth and finally, the Criminal Spam Act prohibits registering for multiple email accounts or Internet domain names, and sending bulk email from those accounts or domains. This provision targets deceptive "account churning," a common outlaw spammer technique that works as follows. The spammer registers, usually by means of an automatic computer program, for large numbers of email accounts or domain names, using false registration information, then sends bulk spam from one account or domain after another. This technique stays ahead of ISP filters by hiding the source, size, and scope of the sender's mailings, and prevents the email account provider or

domain name registrar from identifying the registrant as a spammer and denying his registration request. Falsifying registration information for domain names also violates a basic contractual requirement for domain name registration.

Penalties for violations of these provisions are tough but measured. Recidivists and those who send spam in furtherance of another felony may be imprisoned for up to five years. Large-volume spammers, those who hack into another person's computer system to send bulk spam, and spam "kingpins" who use others to operate their spamming operations may be imprisoned for up to three years. Other offenders may be fined and imprisoned for no more than one year. Convicted offenders are also subject to forfeiture of proceeds and instrumentalities of the offense.

In addition to these criminal penalties, offenders are also subject to civil enforcement actions, which may be brought by either the Department of Justice or by an ISP. Civil remedies are important as a supplement to criminal enforcement for several reasons. First, bringing cases against outlaw spammers is very resource intensive because of the extensive forensic work involved in building a case: providing for civil enforcement will allow ISPs to assemble evidence to make prosecutors' jobs easier. Second, although criminal prosecutions are a critical deterrent against the most egregious spammers, the Justice Department is unlikely to prosecute all outlaw spam cases; civil enforcement, backed by strong financial penalties, will serve as a second layer of deterrence. Third, criminal penalties may not be appropriate in all cases, as for example in the case of teenagers hired by professional outlaw spammers to send out email for them; civil enforcement gives the Justice Department a more complete and refined range of tools to address specific outlaw spam problems.

That describes the main provisions of our bill. In addition, because commercial email can be, and is being, sent from all over the world into the virtual mailboxes of Americans, the bill directs the Administration to report on its efforts to achieve international cooperation in the investigation and prosecution of outlaw spammers.

Again, the purpose of the Criminal Spam Act is to deter the most pernicious and unscrupulous types of spammers—those who use trickery and deception to induce others to relay and view their messages. Ridding America's inboxes of deceptively delivered spam will significantly advance our fight against junk email. But the Criminal Spam Act is not a cure-all for the spam pandemic.

The fundamental problem inherent to spam—its sheer volume—may well persist even in the absence of fraudulent routing information and false identities. In a recent survey, 82 percent of

respondents considered unsolicited bulk email, even from legitimate businesses, to be unwelcome spam. Given this public opinion, and in light of the fact that spam is, in essence, cost-shifted advertising, it may be wise to take a broader approach to our fight against spam.

One approach that has achieved substantial support is to require all commercial email to include an "opt out" mechanism, that is, a mechanism for consumers to opt out of receiving further unwanted spam. At the recent FTC forum, several experts expressed concerns about this approach, which permits spammers to send at least one piece of spam to each email address in their database, while placing the burden on email recipients to respond. People who receive dozens, even hundreds, of unwanted emails each day would have little time or energy for anything other than opting-out from unwanted spam.

According to one organization's calculations, if just one percent of the approximately 24 million small businesses in the U.S. sent every American just one spam a year, that would amount to over 600 pieces of spam for each person to sift through and opt-out of each day. And this figure may be conservative, as it does not include the large businesses that also engage in online advertising.

A second possible approach to spam—a national "Do Not Spam" registry—raises a different but no less difficult set of concerns. The two FTC Commissioners who testified last month at the Senate Commerce Committee's hearing on spam both questioned the potential of a national registry to alleviate the spam problem. Although this approach would place a smaller burden on consumers than would an opt-out system, it would entail immense costs, complexity, and delay, all of which work in the spammers' favor.

A third way of attacking spam—and one that was favored by many panelists and audience members at the FTC forum—is to establish an opt-in system, whereby bulk commercial email may only be sent to individuals and businesses who have invited or consented to it. This approach has strong precedent in the Telephone Consumer Protection Act of 1991. TCPA, which Congress passed to eliminate similar cost-shifting, interference, and privacy problems associated with unsolicited commercial faxes. The TCPA's ban on faxes containing unsolicited advertisements has withstood First Amendment challenges in the courts, and was adopted by the European Union in July 2002.

I have discussed three possible approaches to the spam problem, and there are several others, some of which have already been codified in state law. I encourage the consideration of all these anti-spam approaches in the weeks and months to come.

Reducing the volume of junk commercial email, and so protecting legitimate Internet communications, will

not be easy. There are important First Amendment interests to consider, as well as the need to preserve the ability of legitimate marketers to use email responsibly. If Congress does act, it must get it right, so as not to exacerbate an already terribly vexing problem.

The Criminal Spam Act is a first step in countering spam. If we can shut down the spammers who use deception to evade filters and confuse consumers, we will give the next generation of anti-spam technologies a chance to do their work. Our bill targets the most egregious offenders, it provides a much-needed federal cause of action, and it allows the states to continue to serve as a "laboratory" for tough anti-spamming regulation. I urge its speedy enactment into law.

By Mrs. MURRAY (for herself, Mrs. BOXER, Ms. CANTWELL, Mr. KENNEDY, Mr. LEAHY, and Mr. PRYOR):

S. 1294. A bill to authorize grants for community telecommunications infrastructure planning and market development, and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mrs. MURRAY. Mr. President, I rise today to introduce legislation to help rural and underserved communities across the country get connected to the information economy.

Today I am introducing the Community Telecommunication Planning Act of 2003. I am proud to have Senators BOXER, CANTWELL, KENNEDY, LEAHY, and PRYOR as original cosponsors. This bill will give small and rural communities a new tool to attract high speed services and economic development.

Representative INSLEE by his home State, along with several other members, will soon introduce a companion bill in the House. I appreciate him working with me to meet this challenge.

I am especially proud of how this legislation came about. For the last four years, I've been working with a group of community leaders in Washington State to find ways to help communities get connected to advanced telecommunications services.

I want to take a moment to thank the members of my Rural Telecommunication Working Group for their hard work on this bill. The members include: Brent Bahrenburg, Gregg Caudell, Dee Christensen, Dave Danner, Louis Fox, Tami Garrow, Larry Hall, Rod Fleck, Ray King, Dale King, Terry Lawhead, Dick Liarman, Jim Lowery, Jim Miller, Joe Poire, Skye Richendrfir, Ted Sprague, Jim Schmitt, and Ron Yenney.

We met as a working group, and we held forums around the State that attracted hundreds of people. We've tapped the ideas of experts, service providers and people from across the State who are working to get their communities connected. The result is this legislation, which I am proud to say is

part of Washington State's contribution to our national effort to connect all parts of our country to the Internet.

The bill was originally introduced in the 107th Congress. I was able to attach a version of it to the Farm Bill. Unfortunately, the provision was removed during Conference.

This bill addresses a real need in many communities. While urban and suburban areas have strong competition between telecommunications providers, many small and rural communities are far removed from the services they need.

We must ensure that all communities have access to advanced telecommunications like high speed Internet access and the wireless Internet. Just as yesterday's infrastructure was built of roads and bridges, today our infrastructure includes advanced telecom services.

Advanced telecommunications can enrich our lives through activities like distance-learning, and they can even save lives through efforts like telemedicine. The key is access. Access to these services is already turning some small companies in rural communities into international marketers of goods and services.

Unfortunately, many small and rural communities are having trouble getting the access they need. Before communities can take advantage of some of the help and incentives that are out there, they need to work together and get through a community planning process. Community plans identify the needs and level of demand, create a vision for the future, and show what all the players must do to meet the telecom needs of their community for today and tomorrow. These plans take resources to develop, and my bill would provide those funds.

Providers say they're more likely to invest in an area if it has a plan that makes a business case for the costly infrastructure investment. Communities want to provide them with that plan, but they need help developing it. Unfortunately, many communities get stuck on that first step. They don't have the resources to do the studies and planning required to attract service. So the members of my Working Group came up with a solution: have the Federal Government provide competitive grants that local communities can use to develop their plans. I took that idea and put it into this bill.

After determining what services they need, communities must then go out and make a market case to providers. That is why I've added "market development" to the list of allowable uses of grant funding.

While this bill deals with new technology, it's really just an extension of the infrastructure support the federal government traditionally provides to communities.

The Federal Government already provides money to help communities plan other infrastructure improvements—everything from roads and bridges to

wastewater facilities. Because today's economic infrastructure includes advanced telecom services, I believe the Federal Government should provide similar support for local technology infrastructure.

In summary, this bill would provide rural and underserved communities with grant money for creating community plans, technical assessments and other analytical work, and it would allow these communities to use the funding to market these plans to providers.

With these grants, communities will be able to turn their desire for access into real access that can improve their communities and strengthen their economies. This bill can open the door for thousands of small and rural areas across our country to tap the potential of the information economy.

I urge the Senate to support this bill, and I look forward to working with my colleagues to see it passed.

I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1294

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

"This Act may be cited as the "Community Telecommunications Planning Act of 2003".

SEC. 2. COMMUNITY TELECOMMUNICATIONS PLANNING GRANTS.

(a) **AUTHORITY TO MAKE GRANTS.**—Each Secretary concerned may, using amounts authorized to be appropriated by the applicable paragraph of subsection (g), make grants to eligible entities described in subsection (b) for the community telecommunications infrastructure planning and market development purposes described in subsection (c).

(b) **ELIGIBLE ENTITIES.**—An entity eligible for a grant under this section is any local or tribal government, local non-profit entity, cooperative, public utility, or other public entity that proposes to use the amount of the grant for the community telecommunications infrastructure planning and market development purposes described in subsection (c).

(c) **COMMUNITY TELECOMMUNICATIONS INFRASTRUCTURE PLANNING AND MARKET DEVELOPMENT.**—Amounts from a grant made under this section shall be used for purposes of facilitating the development of a telecommunications infrastructure and market development plan for a locality by various means, including—

(1) by encouraging the involvement in the development of the plan of interested elements of the community concerned, including the business community, governments, telecommunications providers, and secondary and, where applicable, post-secondary educational institutions and their students;

(2) by enhancing the focus of the development of the plan on a wide range of telecommunications needs in the community concerned, including needs relating to local business, education, health care, and government;

(3) by enhancing the identification of a wide range of potential solutions for such needs through advanced telecommunications infrastructure; and

(4) by any other means that the Secretary concerned considers appropriate.

DOCUMENT NO. 6