Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of:	)	
	)	
CAN-SPAM Act Rulemaking	)	Project No. R411008

COMMENTS OF VERIZON[1]

The Commission should recommend against the adoption of a national do-not-e-mail registry and should not exercise its discretionary authority to implement such a registry. The idea behind a national do-not-e-mail list – protecting consumers from receiving unwanted and misleading e-mail – is laudable. In reality, however, the registry would undermine the very purpose it seeks to serve, engender confusion and dissatisfaction, and impose excessive burdens on legitimate users of e-mail marketing. Thus, Verizon agrees with Chairman Muris that "[t]here is no basis to conclude that a Do Not Spam list would be enforceable or produce any noticeable reduction in spam."[2]

As a company that provides Internet connectivity to millions of customers, Verizon is a strong opponent of spam. For example, in 2002, Verizon Online (Verizon's Internet service provider) concluded a highly visible civil prosecution of Alan Ralsky, a notorious alleged spammer. Verizon Online, through its individual efforts and collectively as a leader in industry

[1] These comments are submitted on behalf of Verizon Internet Services Inc. and GTE.Net LLC d/b/a Verizon Internet Solutions (which operate under the trade name Verizon Online) as well as Verizon's affiliated local exchange carriers and long distance companies (with Verizon Online, collectively referred to herein as "Verizon"). Some of these companies are service providers subject to regulation under the Communications Act of 1934, as amended, and therefore are subject to the enforcement jurisdiction of the Federal Communications Commission, not the FTC. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), § 7(b)(10), P.L. 108-187, 117 Stat. 2699.

[2] Remarks of Timothy J. Muris, Chairman, Federal Trade Commission, before the Aspen Summit, Cyberspace and the American Dream, Progress and Freedom Foundation, August 19, 2003 ("Aspen Remarks").

organizations such as the U.S. Internet Service Providers Association ("USISPA") and the Internet Commerce Coalition (the "ICC"), has actively and aggressively lobbied in favor of stronger civil and criminal penalties for violations of federal and state anti-spam laws. Verizon played an important role in the passage of the recent amendments to the Virginia anti-spam law, *see* Va. Code § 18.2-152.3.1 (2003), and has also been a frequent proponent of other state laws and a commentator on drafts of the CAN-SPAM Act. In addition, Verizon Online, like other major ISPs, fight a continuous battle against unwanted commercial email because of the burden it places on Verizon's ISP customers and the costs it imposes on Verizon's network (e.g., network over-engineering and the purchasing, installation and support of anti-spam filtering technologies). For all these reasons, Verizon strongly supports Congress's and the FTC's efforts to curb unwanted and misleading e-mails.[3]

A national do-not-e-mail registry, however, is not the answer to the spam scourge. The "practical, technical, security, privacy, enforceability, or other concerns" associated with such an endeavor cannot "be overcome so that a registry would be workable and effective." *Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act*, Advanced Notice of Proposed Rulemaking, at 26. Accordingly, the Commission should decline to exercise its discretionary authority to implement a do-not-e-mail list, and should issue a report to Congress recommending against the adoption of such a list. CAN-SPAM Act, §§ 9(a), 9(b).

[3] Congress recognized that many ISPs are "undertaking extensive investigative and legal efforts to track down and prosecute those who send the most spam, in some cases, spending over a million dollars to find and sue a single, heavy-volume spammer." *See* Senate Report 108-102, to accompany S. 855, at 6, July 16, 2003.

I. THE DO-NOT-EMAIL REGISTRY RAISES IMPORTANT SECURITY AND PRIVACY CONCERNS AND MAY INADVERTENTLY PROVIDE SPAMMERS WITH A "GOLDEN" LIST OF EMAIL ADDRESSES.

A national do-not-e-mail registry threatens to undermine rather than protect the security and privacy of consumers who submit their email addresses to the registry. There is no way to keep outlaw spammers from obtaining the list – which could contain tens or hundreds of millions of valid e-mail addresses. Distributing such a list in any form will inevitably place in the hands of spammers a "golden" list of email addresses. Indeed, a ready-made compilation of valid e-mail addresses would be of incalculable value to spammers, who otherwise must expend considerable efforts to create their own such lists. As Senator Wyden (one of the key sponsors of the CAN-SPAM Act) cautioned, "We all understand that if a bad spammer, for example, one of the kingpin operators, was to [obtain a national e-mail registry], what a gold mine for an evil person who wanted to exploit our citizens." Remarks of Sen. Wyden, S13027, Congressional Record, Oct. 22, 2003.

To be effective, the do-not-email list would need to be made available to marketers (emailers) who intend to comply with it. However, Verizon in not aware of any truly effective way to allow access to legitimate emailers while denying access to spammers. While industry groups may tout encryption and other techniques for assuring the security of the list, outlaw spammers have already demonstrated little or no respect for the law. If a registry list were ever to be created, in any form, it would quickly propagate to the spammer community, which in turn would be armed with a goldmine of validated addresses. Thus, the underlying goal of the registry list – to compel emailers to scrub their email lists against the list of excluded addresses – ultimately would result in an *increase* in spam.

Experiences with the national do-not-call list are not a valid predictor of the potential success of a do-not-email list. A do-not-e-mail list is far more susceptible to abuse than a do-not-call list. Disclosure of a list of telephone numbers, while certainly creating the potential for misuse, has far more limited effect because exploiting the list would impose significant costs (telecommunications charges) on the marketer. In contrast, the marginal cost of sending e-mail is essentially zero.[4] In addition, the fluid nature of email means that a list of addresses, once in the stream of commerce, is capable of immediate and widespread dissemination. It takes little technical skill or effort for a spammer to convert such a list to its own illicit purposes.[5]

Requiring companies to keep their own do-not-e-mail lists (as is mandated by § 5(a)(4) of the CAN-SPAM Act) better protects the integrity of those lists and minimizes the risk of unauthorized distribution. Rigorous civil and criminal enforcement by law enforcement, and private enforcement actions by the ISP industry under the CAN-SPAM Act and state anti-spam laws, coupled with email authentication, ISP and end user blocking, and filtering techniques, are the most effective ways to safeguard consumer privacy while continuing the battle to control spam.

---

[4] As Chairman Muris has explained, during the FTC's "Spam Forum, a bulk emailer testified that he could profit even if his response rate was less than 0.0001%. Because there is virtually no marginal cost to increasing the number of messages, fraud artists and pornographers, who generally have little to gain from reputation, profit from extremely low response rates by sending untold millions of messages." Aspen Remarks, Section III.E.

[5] Requiring commercial e-mail senders to submit their own lists to the registry for scrubbing against the national list would not diminish abuse. Rather, spammers could increase their use of "dictionary attacks" in order to determine which e-mails on their lists were valid. In particular, they would (1) generate lists of e-mails addresses using random combinations of names, letters, and numbers, (2) submit their lists to the registry (which would remove only the valid, registered e-mail addresses from the spammers' lists), and (3) compare the "scrubbed" list received from the registry with their original lists in order to determine which addresses on their original lists were valid. Indeed, the existence of a national registry makes such dictionary attacks more attractive to spammers; currently, spammers must send millions of messages and wait to receive bounce backs from invalid addresses to determine which are valid.

II. IMPLEMENTATION OF A NATIONAL DO-NOT-EMAIL REGISTRY RAISES SERIOUS ENFORCEABILITY CONCERNS THAT WILL UNDERMINE PUBLIC CONFIDENCE IN THE REGISTRY.

Compliance with a national do-not-email registry would not be enforceable as a practical matter, and moreover, may exacerbate the public perception that spam is an insolvable problem and undermine public confidence in the registry. Spam can be – and is – generated from anywhere in the world, and the web sites advertised through spam likewise can be located anywhere in the world. According to the Senate Committee Report for the CAN SPAM legislation, only 11 percent of spam originates in North America; approximately 60 percent comes from IP addresses assigned to Europe (including 10-12 percent from Russia alone), and 16 percent originates in Asia (with China leading that region).[6]

The most serious spammers can easily mask their identity and will continue to send spam regardless of any legal considerations. As Chairman Muris has explained:

> Email can be sent from anywhere to anyone in the world, without the recipient knowing who sent it. Spammers are technologically adept at hiding their identities, using false header information, and routing their emails across borders and through open relays, making it extremely difficult even for experienced government investigators with subpoena power to track them. Our enforcement experience, and that of the few states that have tried to punish spammers, is that it can take months of investigation, and the issuance of a dozen or more subpoenas, simply to locate a spammer. Although we are dedicating significant resources to attacking deceptive spam, it is difficult to prosecute enough spammers to have a serious deterrent effect, let alone stop, or even slow down, the problem. Aspen Remarks, Section III.E.

[6] *See* Senate Report 108-102, to accompany S. 855, at 5, July 16, 2003. Indeed, more and more spam is originating overseas, with China fast becoming an even more significant major spam hub than the statistics cited in the Senate Report. *See* Mike Wendland, "Spam King Lives Large off Others' E-Mail Troubles, West Bloomfield Computer Empire Helped by Foreign Internet Servers," http://www.freep.com/money/tech/mwend22_20021122.htm.

Indeed, one of the central tenets of the CAN-SPAM Act was to provide a federal vehicle for attacking the "outlaw" spammer – those who engage in the most serious forms of misrepresentation and evasion.[7]

Establishing a supposed safeguard against spam, but then being unable effectively to enforce compliance against off-shore spammers and those who thwart detection, would be more harmful to consumer expectations of privacy than not setting up the safeguard at all.[8] Creating the impression that submitting one's email address to the registry will halt *all* unsolicited email is setting an expectation that cannot be met. Outlaw spammers ignore the law today. They will ignore the registry tomorrow. Consumers who submit their email addresses to the registry will have the reasonable expectation that the registry will work – as is the case with the do-not-call registry. When unwanted emails continue, as they inevitably will, these consumers will become distrustful of the registry and the FTC's ability to control the spam problem. This eventuality benefits neither the consumer nor the agency.

III. THE DO-NOT EMAIL REGISTRY RAISES SIGNIFICANT PRACTICAL AND TECHNICAL CONCERNS.

---

[7] *See* CAN-SPAM Act, §§ 4, 7, 11; *see also* Remarks of Sen. Wyden, S13037, Congressional Record, Oct. 22, 2003 ("The bottom line is that when this bill becomes law, big-time spamming, in effect, becomes an outlaw business. For the first time, the kingpin spammers are going to be at the risk of federal prosecution, Federal Trade Commission enforcement, million-dollar lawsuits by State attorneys general and Internet service providers"); Remarks of Sen. Hatch, S13029, Congressional Record, Oct. 22, 2003 (the Act "includes stiff penalties intended to deter the most abusive spammers. Recidivists and those who send spam [] commit another felony [and] face up to 5 years' imprisonment. Those who hack into another's computer system to send spam, those who send large number of spam, and spam kingpins who direct others in their spam operations, face up to 3 years' imprisonment"); Remarks of Sen. Leahy, S13043, Congressional Record, Oct. 22, 2003 ("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 3 years").

[8] *Cf. Honig v. Doe*, 484 U.S. 305, 311 n.1 (1988) (noting that Congress has rejected policies of "merely establish[ing] an unenforceable goal"); *see also Gary B., v. Cronin*, 542 F. Supp. 102, 109 (N.D. Ill. 1980) ("It can no longer be the policy of the Government to merely establish an unenforceable goal") (quoting Senate Report to Pub.L. 94-142, § 3(c), 89 Stat. 775 (1975)).

Maintaining and complying with a national do-not-e-mail registry would be extremely difficult for legitimate marketers – certainly, much more so than maintaining and complying with the national do-not-call registry. While most people have only one or two phone numbers, it is not unusual for consumers to have many more e-mail addresses. If only a portion of those addresses were registered (whether through inadvertence or on purpose), consumers would continue receiving unwanted e-mail at unregistered email addresses. In addition, consumers change e-mail addresses far more frequently than they change phone numbers[9]; e-mail addresses, unlike phone numbers, are not portable, and customers regularly switch ISPs.[10] As a result, maintaining an accurate do-not-e-mail list, and assuring compliance with that list, would require constant updating of the registry and downloads by marketers attempting to comply with it.[11]

Additionally, complying with the national registry would be exceptionally burdensome for legitimate marketers. Verizon already maintains company-specific do-not-e-mail lists and cross-checks prospective e-mail recipients against these lists to assure compliance. These lists are compiled in several ways, including responses to targeted solicitations and opt-out requests on company websites and during service registration by the customer. If a current or potential customer elects not to receive email from a Verizon entity, or opts out of receiving future emails,

[9] As Senator Wyden observed, "people change their e-mail addresses constantly. In that sense, this is different than a telephone." Remarks of Sen. Wyden, S13027, Congressional Record, Oct. 22, 2003.

[10] To the extent e-mail addresses are recycled, there could also be a significant problem with addresses remaining on the list without the new "owner" of that address even being aware of that fact. The only effective way to address this problem is to either require consumers periodically to update their email address in the registry or to have "registered" addresses time-out after a defined period.

[11] In addition, because e-mail addresses (unlike phone numbers) vary in length and character make-up, there is an increased risk that such addresses will be entered inaccurately into the registry. Care would need to be taken to ensure consumers correctly enter their email address, such as confirmation emails to registering consumers.

Verizon respects the individual's request as the CAN-SPAM Act and Verizon's own email and privacy policies require. Accordingly, maintaining a company-specific do-not-email list is an obligation with which Verizon is fully prepared to, and does, comply.

In contrast, if Verizon had to cross-check its e-mails against a list with potentially hundreds of millions of addresses (the vast majority of which pertain to consumers not in Verizon's serving territory or who are not subscribers to Verizon services), the costs of compliance would be exponentially greater. For Verizon, as for every other legitimate e-mail marketer, the increased costs of compliance ultimately would have to be reflected in the prices for its services and products.

IV. A NATIONAL DO-NOT-EMAIL REGISTRY MAY LEAD TO OVERLY BROAD EXCLUSIONS AND UNINTENDED, ADVERSE CUSTOMER CONSEQUENCES.

Like many companies, Verizon often communicates important service-related and billing information to its customers by email. In fact, Verizon reserves the right to communicate service-affecting messages via email both in its opt-out selection process and in its Verizon Online terms of service. A national do-not-email registry would unduly limit Verizon's ability to communicate important information to its customers, thereby placing customers at risk of not seeing account-related information or imposing significant mailing costs on Verizon if an email option is no longer available.

Moreover, if consumers receive legitimate service—or account-related emails after they have registered—they may believe that the sender has violated their request not to receive emails from any source. The registry will understandably create in the consumer's mind an expectation that, by registering his or her email, *no* commercial email will be received. While the registry may make clear that registering an email address will not prohibit service-related or

"relationship" emails, consumers may not understand the subtlety of this distinction. The CAN-SPAM Act creates a useful and, with appropriate clarification by the FTC in future rulemaking proceedings,[12] functional dichotomy between "advertising" and "relationship" emails. The Act also creates a workable mechanism for recognizing and respecting consumer consent to receive emails, and requirement for removal of that consent. CAN-SPAM Act, § 5(a)(4). The lines between these categories of email would become unnecessarily blurred *in the consumer's mind* if the national registry were implemented.

In addition, not all email is unwelcome or offensive. If an advertiser follows the labeling and opt-out requirements of the law, it should be permitted to send email to consumers it reasonably believes have an interest in receiving information about the sender's services or products. Indeed, a recent Pew study revealed that more than two-thirds of consumers surveyed do not consider unsolicited commercial e-mail from senders with whom they previously have done business to constitute "spam." PEW Internet and American Life Project, "Spam: How It Is Hurting Email and Degrading Life on the Internet," at 10 (Oct. 22, 2003). And, that same study disclosed that one-third of consumers have responded to solicitations contained in unsolicited commercial e-mails, and seven percent have ordered a product that was offered in such an e-mail. *Id.* at 25. Consequently, by registering their email address(es), consumers may be foreclosing their ability to receive emails that they would have an interest in viewing.

---

[12] *See* CAN-SPAM Act, § 3(2)(C)(directing the FTC to engage in a rulemaking to define the meaning of the phrase, "primary purpose," in the definition of "commercial electronic mail message"). Among other things, this proceeding should further define the parameters between commercial "advertising" and "relationship" emails. *Compare* CAN-SPAM Act, § 3(2) (defining "commercial electronic mail message") *with id*., § 3(17) (defining "transactional or relationship message" and giving the FTC authority to modify the statutory definition "to expand or contract the categories of messages that are treated as transactional or relationsh8ip messages … to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of the Act").

Finally, it bears repeating that the registry will only keep *legitimate* emailers from sending email targeted to consumers who register with the national do-not-email list. The outlaw spammer, who today flaunts the law, will continue to do so, with or without a registry. Offensive or misleading emails will continue to be sent, and only marketers who attempt to follow the law will be penalized.

V. CONCLUSION

For the foregoing reasons, the FTC should not exercise its discretionary authority to implement a national do-not-e-mail registry and should recommend to Congress that such a registry not be mandated.

VERIZON

By: /s/ Jeffrey S. Linder

Jeffrey S. Linder
Rebekah P. Goodheart
WILEY REIN & FIELDING LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000

Michael E. Glover
Edward Shakin
Ann H. Rakestraw
VERIZON
1515 N. Courthouse Road
Suite 500
Arlington, VA 22201
(703) 351-3174

Thomas M. Dailey
Verizon Internet Services Inc.
1880 Campus Commons Drive
Reston, VA 20191
(703) 295-4285

Its Attorneys

March 31, 2004