Observations: Sending unsolicited bulk email (UBE) has never been an accepted practice on the internet. Persons who send UBE, and those who host them are not prone to voluntary cooperation for the purpose of maintaining the usefulness of the internet, in particular email, for anyone other than themselves. Indeed, as observed by the FTC in the past, they are often criminal. Because the sending of UBE has never been an accepted practice a do not email registry (DNER) cannot be used in good faith. Persons acting in good faith and respecting the wishes of the recipient will not send UBE, and therefor have no use for a do not email list. The expressed consent of the recipient must supercede the presence of their email address on a DNER and legitimate senders of bulk email send only to those for whom they have received consent. The only reliable protection against UBE is anonymity of the recipient. If the sender of UBE cannot obtain or guess a recipient's email address then the sender cannot send that recipient email. Even if a do not email registry could be used in good faith, it cannot be used at all unless it is published in some manner. Even if the list per se is kept secure, senders must be able to compare their own lists to the DNER, or have it compared for them and thus be informed directly which email addresses are to be removed or will be able to deduce which have been removed from a cleaned list by differencing the cleaned list with the uncleaned. Email addresses that have been determined to be on the DNER can then be sold clandestinely, or outside of the jurisdiction of the United States, sold openly as 'confirmed email' addresses. Seeding the DNER with 'spamtraps', addresses unique to the DNER, will not protect against this as those spamtraps will not be on the senders' lists submitted for comparison. Even when an abuse of the DNER is identified, prosecution of the abuser may well be impossible due to jurisdictional issues. Much of the UBE received by Americans today is sent from outside of the United States, beyond the reach even of the discovery needed to provide evidence beyond circumstance of a link to American interests. Because the FTC cannot assure, through technology or law, that the DNER will not be used abusively, individuals would be well- advised to not submit their email addresses to the list, depending instead on the only reliable protection, anonymity. It is further observed that the legitimate registered owner of a domain name has certain rights to permit or restrict use of the domain name as established by custom and law. Recommendations: In view of the above facts, two imperatives emerge. 1) The fact that an email address does not appear on a do not email registry (DNER) must not be interpretted as _de facto_ permission to send unsolicited bulk email (UBE) to that address. It is practically, legally, and morally unfeasible to require that an individual wishing to assert their right to be free from UBE forfeit that right by declining to participate in a program that by its very nature renders them more vulnerable to abuse of that right. To do so is tantamount to requiring that banks publish the combinations to their vaults in order to secure legal protection from bank robbery. 2) Any DNER must permit blanket or universal opt-out of all email addresses for a particular domain at the sole discretion of the proper registered owner of that domain. Aside from the basic principle that the legitimate owner of property, real or virtual, should be able to choose how and by whom that property is used this is the only approach to maintaining a DNER that permits participation by an individual (through their choice of domain) while also permitting them to retain anonymity of their email address. Douglas S Caprette[redacted] Greenbelt, MD[redacted]