Unfortunately, no there are no statistics I can offer that I am aware of. To my knowledge there are no papers on the suggestion.

The comment and suggestion arise out of personal experience. Not only am I conducting my own business via internet but I am also Vice President of a very small organization for other businesses within the same industry (Society of Independent Representatives).

My own business relies upon cable internet connection provided by the well known Road Runner system. This places my business email at the mercy of a very large independent IP. The consequence of this is that frequently, another customer of RR will violate internet courtesy and spam controls and rr.com or neo.rr.com will be placed into one of the innumerable Spam lists. Then my business email communication is interrupted by non-delivery to my client or associate. Such an incident occurs typically once per month and requires at a minimum 3 days communications to my IP to resolve. My clients are typically large business enterprises - lenders, bankers, etc. and my associates are typically other micro-business and/or small businesses many of whom operate from a home office as I do and use their home IP service for business communications.

The organization faces a different but similar problem. E-mail for the organization is processed through a virtual server. The majority of email sent out is to opt-in subscribers and business members of the organization. These contacts are 3000+ in number and range from the micro-business to the large business enterprise such as the lender or government agencies such as HUD. The organization adheres to a strict opt-in/opt-out policy and typically has daily communications to the membership and monthly communication to mailing list subscribers. Again, the organization, relying on a third party, is at the mercy of compliance of the IP's other clients. Mail delivery is interrupted less frequently and requires a minimum of 7 days to resolve depending on which Spam list has placed a block.

Daily incoming email can reach 500+ in volume. With a variety of spam filters in place, 75% or more is still blatant spam, scam-spam, porn-spam or virus infected. This mornings percentage was 90% spam oriented. 2% virus. 8% business.

The suggestion provided would create a minimal impact on small and micro-businesses and is financially feasible for all business entities. It could be accomplished with the creation of a few (knowledgeable) IT positions within any regulatory entity. It would require a large and fully capable networked database.

For many businesses, registration could take place at the time of domain selection. The business purchasing a domain would only need to register their domain email address such as @xyzcompany.com Private and dedicated server IP addresses could logged during the registration of the network. Virtual servers (such as what our organization uses) often do not have dedicated IP addresses and would prove a small exception to the registration process. The domain email addresses could be registered but the IP left as a variable. Micro-business, such as myself, would need to register with the email address and business entity using it. More often than not, especially for a micro-business with dial-up, there is no specific IP correlated to the business entity. Registration could be set as a part of the internet service purchase and email address selection.

By registering, the business would be committing themselves to a Best Practices policy. The one that our organization uses is fairly straight forward: One introduction letter email is sent to each new e-mail address referred to the organization and not again for a period of 12 months - all email is automatically logged with a last email date. E-mail is sent to anyone requesting communication. Bulk e-mail to subscribers always contain notification that the recipient requested the information and information on how to un-subscribe. Anyone requesting removal is immediately removed and that email address is maintained in the database with a block on it. We do not sell our database or the email addresses it contains.

As the organization maintains an on-line directory containing over 1000 email addresses, the website's visitor logs are checked regularly (about 4 times per month) and any IP that is recorded and appears to have been scraping the directory for email addresses is blocked from future access to the website. There

are currently about 15 IP addresses blocked from site access - all resolve to a foreign country. We have a terms of usage policy for the on-line directory.

Voluntary compliance of course has presented the current situations with spam. But placing the burden on the small and micro-business of having to refer to and import regularly large-scale "do not e-mail" lists would be cost prohibitive to the micro-business and certainly an enormous strain on the small business. B2B of the micro-business could possibly evaporate.

With a registry of compliant businesses, another business or private individual could send a complaint directly to the registry rather than having to locate the IP, host, or registrar of the domain name. I would imagine most private individuals do not even know how to obtain complete electronic headers or the procedures for locating the abuse department for the multitude of Internet Providers. The registry would streamline the complaint process as the spam receiver would only need to copy the "from" email address and forward on the complaint to the registry.

The registry would either have the business listed or not. If the business were listed, an email or real letter could be forwarded to the offender. The registry would have the authority to strip Internet privilege for a blatant non-compliant business. However with the infrequent instances of complaints against any particular registered business - some form of incremental warnings could be provided and privilege stripping enforced only if the complaints reached a certain volume or created a discernable pattern.

Problems could arise with instances of forged headers. However, it has been my personal experience that when forged headers are utilized by one party, there is always a clear and undeniable link to a website within the email message body. My personal experience has been that these businesses thrive on some form of independent sales agent who bears the sole responsibility of the spam while the domain business is allowed to continue. In these instances, the registry should enforce the compliance on the profiting business who would be required to register the business domain and it would be the profiting business who would be bound to a Best Practice protocol regardless of whom their sales agents were or what practices their sales agents employed. Placing this burden on the profiting business, in my opinion, would put the dampers on the "we did not do it" escapism tactics.

The entire concept of internet business thrives on the boundary-less opportunities of the world wide web. Typically, I can sit here in my home office and have a client or customer in Japan. I also have the ability to solicit, under a Best Practice Policy or wanton disregard for one, anyone in the world. This ability and choice creates a unique atmosphere where local law and regulation is nearly pointless and where any local law or regulation has the potentiality of creating a financial crisis to my business.

Creation of a world wide web regulatory body of international scope is far more feasible by means of a registry for the business rather than a registry of the private individual. Email addresses are disposable products for the consumer. Business, on the other hand, typically take their email address and/or domain name as an extension of their business name. For instance, my company is Rose's Property Maintenance Service and my email is rosespms@neo.rr.com I have had this email address for seven years. The organization that I have referred to has the domain sirs4quality.org combining both the business name and purpose into the domain name.

The private consumer, on the other hand, (due to the advice of so many authorities on spam and the ease of changing internet providers) may change their email address every month to either alleviate spam or to obtain a less expensive provider. Johnny Public may have the email address of jpublic@aol.com one day and the very next day have jpublic1@msn.com or even j1public@aol.com Which translates that daily Johnny Public must enter his new email address into a "do not spam" registry which then must be daily down-loaded, imported and cross-referenced by each and every business conducting internet transactions. (As a micro-business, my database would not be able to bear this load.)

Unlike telephone numbers which the typical household maintains one or two uniquely for an indeterminate length of time, email addresses are typically provided in groupings of 5 or more to each customer of internet service free of charge with the service. Email addresses are not unique. At any time,

even with the same internet provider, a consumer has the ability to change their email address, request additional email addresses or subscribe to additional free email addresses via Yahoo, Hotmail, MSN or other free providers. So, it is not a set limited number of email addresses per consumer as it is with telephone numbers. A consumer with one telephone number which remains constant could also have 15 or 20 email addresses which could vary exponentially over the singular time frame that the one telephone number remains constant.

If it were the responsibility of a business to enter a registry - the chance of daily change is eliminated. I could register my company once and be good to go for as long as I maintain that business domain or email identity - in my case seven years.

Such proposals as creating .sex .gam .pil and .por for those businesses wishing to engage in (respectively) sexual/adult, gambling, pharmaceutical drugs, and pornography would also create easy email block controls for any business or private party. Of course that is a separate subject and one that needs addressed to ICANN or whomever it is that regulates the domain extensions available.

I respectfully request consideration of the above while your agency is formulating the rules and regulations which my business and innumerable other micro-businesses will need to adhere to.

Thank you
Mimi Norris
Rose's P.M.S.