

Via Email: privacy-noi-2010@ntia.doc.gov

Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce
Room 4725
1401 Constitution Avenue, NW
Washington, DC 20230

Subject: Notice of Inquiry

Ladies and Gentlemen:

This letter responds to the request by the Department of Commerce's Internet Policy Task Force (Task Force) for public comment by Internet stakeholders on the impact of current privacy laws on the pace of innovation in the information economy and whether those laws serve consumer interests and fundamental democratic values.

Who we are

[Zix Corporation](#) is the market leader of email encryption services. We provide secure email services to more than 1,200 hospitals and 1,300 financial institutions, including some of the nation's most influential companies. We also secure email for federal, state and local government organizations, including the United States Treasury Department and the Securities and Exchange Commission.

The Role of Email in Internet Commerce

We agree with the Task Force's statement that "*Commerce today depends on online communication and the transmission of significant amounts of data.*" Global business today is increasingly based on electronic commerce. Online communication and data transfers via the Internet enable commerce at a pace that is increasingly instantaneous and borderless. Much of the information being communicated over the Internet for business and personal use takes the form of electronic mail messages – "email."

Email is a principle consumer and business use of the Internet. According to Wall Street Research, the number of email users worldwide is expected to grow to 1.6 billion by 2011. In the United States, 91% of Internet users have sent or read email online and 56% of Internet users do so daily. Access to the Internet is nearly universal in the U.S., and it is increasingly available to consumers using mobile devices. Email is the main content type accessed by 44% of mobile Internet subscribers via their smart phones.

Email is extraordinarily simple to use, ubiquitous and flexible. There are a variety of email applications for desktop, laptop and mobile devices. Email can be retrieved via an internet browser using a shared computer. Email facilitates the rapid exchange of all types of information in real

time among multiple participants. It also serves as a file transport tool, allowing senders to attach a variety of document formats, images and other files. For all these reasons email has become an integral part of electronic commerce. Email is the primary method that businesses and individuals use to exchange information.

Need for Consumer Confidence in Internet Data Privacy

We agree with the Task Force's statement that "*Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained.*" Moreover, that statement is equally true whether the information is "at rest" on an enterprise's server or "in transit" over the Internet. For electronic commerce to continue to flourish, consumers must have confidence that confidential information they send, receive and store online will remain secure and private.

When consumers purchase goods or services online, their transactions are frequently confirmed and detailed in email receipts. Consumers provide email addresses to subscribe to information delivered periodically by email. Becoming a participant in social media sites or other online communities requires the individual to provide a valid email address and private messages from other users of those sites may be transmitted via email.

Despite their including confidential content, emails in transit are often stored on multiple servers, and the content may be "in the open" so that the message content can be intercepted and viewed by unauthorized persons and used in ways unintended by the sender and recipient. Email senders should, therefore, be encouraged to take steps to ensure that the content of email messages may be read only by the intended recipients.

One proven method of enhancing consumer privacy and confidence in e-commerce is through the use of encrypted email. As described below, new technologies make using encrypted email simple and efficient.

Expectations of Privacy in Email Communications

We note the [comment submitted by Robert Sprague](#), indicating that courts assume that a person loses a reasonable expectation of privacy in email messages once they are sent to and received by a third party (citing *Rehberg v. Paulk*, 598 F.3d 1268 (11th Cir. 2010)). We assert that conclusion should not be true for messages sent via encrypted email, where the sender has taken additional steps to protect the content of the email message and thereby continues to have a reasonable expectation of privacy.

Furthermore, we believe the vast majority of U.S. consumers would be shocked to learn that their email communications are considered by some courts to be less private than a postcard sent via mail. Consumers in the U.S. have reasonable expectations of privacy in the content of their email messages similar to their privacy expectations in telephone communications. For example, the [Electronic Communications Privacy Act](#) and state wiretap laws create the expectation that the content of email communications is secure and private.

In the early days of email services, Internet Service Providers (ISPs) stored messages on their servers only until the user downloaded the message to a personal computer. Once

downloaded, the message was deleted from the server. Increasingly, however, email is being offered as a hosted service by ISPs and others. The content of emails can be stored by the provider indefinitely and accessed by the user remotely “in the cloud,” rather than being downloaded and stored offline.

The fact that emails are increasingly accessed “in the cloud” should not diminish consumers’ reasonable expectation of privacy in those communications. Consumers do not consider their stored emails to be publicly available or “in plain view” whether they are locally downloaded or they are stored on a server operated by an email services provider. They most likely do not expect their email provider to scan the content of their emails to glean insights for targeted behavioral marketing or other purposes not intended by either the sender or recipient.

We also note Mr. Sprague’s observation that current privacy law does not necessarily protect information derived from the accumulation of data. “In other words, when individuals voluntarily relinquish their right to privacy over small, unique pieces of information, an analysis of accumulated data may generate a much fuller profile, which itself is not protected because the underlying data are not protected (citing *Solove, D.* 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy, *Stanford Law Review* 53: 1393-1462).” As we describe below, this is equally true with respect to information aggregated from the content of unsecured emails.

The Scope of Private Data in Email

An email address is unique to the individual or organization that creates it. The discussion [draft privacy legislation](#) published on May 4, 2010 by Representative Rick Boucher, Chairman, and Cliff Stearns, Ranking Member, of the House Energy and Commerce Committee’s Subcommittee on Communications, Technology, and the Internet, recognizes in section 2(5)(D) that an email address should be protected as “covered information” because it can uniquely identify a sender.

The types of “private” information that may be contained in email goes beyond ordinary concepts of Personally Identifiable Information (PII) like a driver’s license number or social security number. In nearly every e-commerce interaction, individuals provide an email address together with their name, address and often their credit card information.

Access to an email account permits one to know a considerable amount of private information about the email account holder. An individual’s email address can become inexorably linked to private details of that individual’s lifestyle and behavior. For example, emails may divulge what medications, products and services the individual purchased online; where and to whom those items were shipped; movies and music they downloaded; travel arrangements they made; books, magazines and newspapers they read; sexual orientation, and their membership in professional, political, religious, ethnic and social groups. An individual’s email account is a portal into that person’s lifestyle. The content of email, individually or in the aggregate, can expose fundamentally private information about the individual.

Contractual usage restrictions and privacy policies, particularly when they may be periodically revised in ways adverse to individual privacy, have not proven to be effective in protecting consumer’s confidential information. Although it is possible for a consumer to “opt out”

by changing to an email provider whose policies are more protective of individual rights, it is impractical for consumers to routinely change email addresses because of the time and effort required to provide the new email address to all of their personal and business contacts, update their website subscriptions, etc. Moreover, the notion of “informed consent” presumes that consumers actually understand how data service providers utilize and re-purpose the personal data that they obtain in providing services, and the implications of how their personal data might be utilized.

Technological privacy solutions are far more effective in protecting individual rights than are policy-based usage limitations.

New Privacy-Enhancing Technologies and Information Management Processes

How Email Encryption Protects Privacy

Data encryption can make the contents of every email, both the message text and any attachments, virtually indecipherable to unauthorized individuals. Encryption uses a complex mathematical equation to convert the original email content into an information package that cannot be read until the intended recipient unlocks the message. Email is encrypted to meet standards set by [The National Institute of Standards and Technology](#), which are deemed adequate to protect the content from malicious individuals. So, as a practical matter, if an unauthorized individual intercepts a copy of an encrypted email while it is moving across the internet or while it is stored in message archives, the unauthorized individual simply will not be able to read the message contents.

The U.S. government and state governments have acknowledged that encryption of email is an effective means of protecting confidential information. For example, a recent [Massachusetts regulation](#) requires for healthcare providers the "encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."

Automated Policy-Driven Email Encryption

A law or policy that relies on employees not to send sensitive information via “open” email is not practically effective to protect consumer privacy. Even if full compliance could be ensured within an enterprise’s own workforce, external participants such as consultants may be tempted to ignore the policy in favor of the convenience and efficiency of email communication.

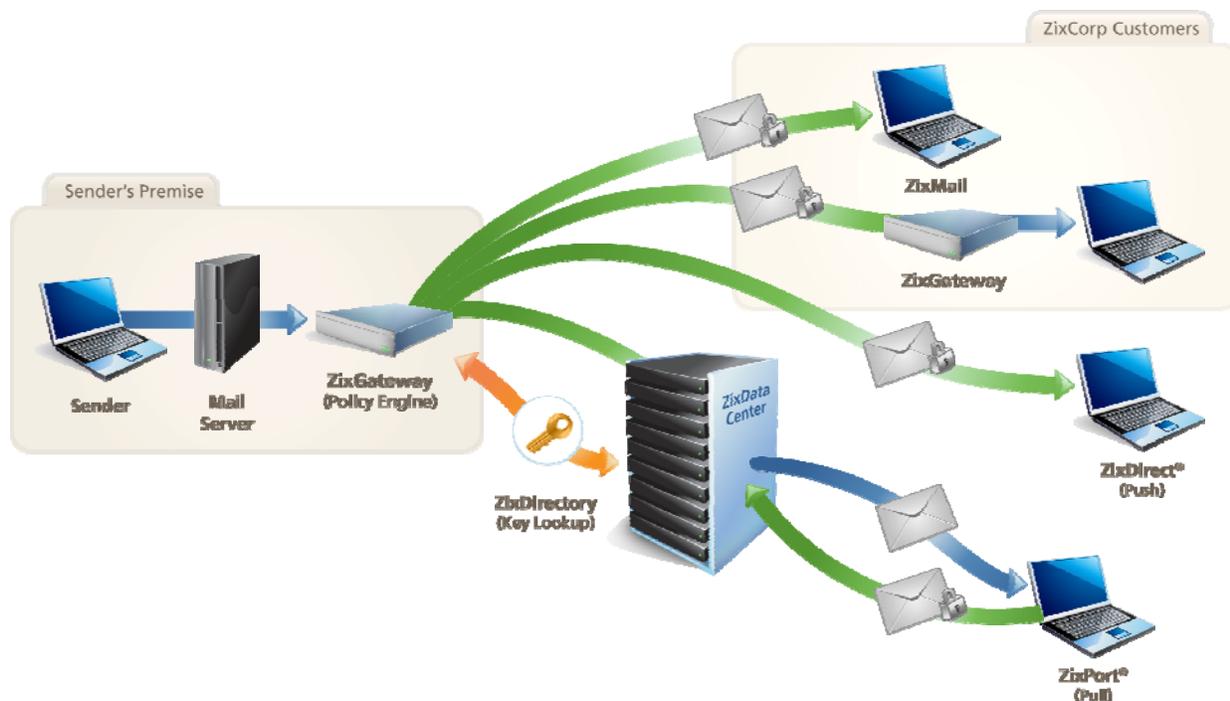
Automated, policy-driven email encryption offers a privacy solution that facilitates compliance with national and state privacy regulations as well as voluntary enterprise practices. An enterprise can adopt a “policy” that prescribes what email must be encrypted based on content, attachments, email address or other factors.

A compliance “lexicon” is developed that examines the message subject, text and non-binary attachments for content that policy dictates should be encrypted for confidentiality – including personal privacy concerns. An electronic appliance on the enterprise’s email server inspects each outbound email and its attachments to see if the adopted policy and lexicon requires

that the message be encrypted. If the policy applies, the appliance automatically encrypts the message before sending it to the recipients.

At an enterprise that uses automated, policy-driven email encryption, the employees do not have to make judgment calls about whether content is private. The employees don't need to remember to secure sensitive email content. Confidential messages are automatically encrypted. Similarly, when encrypted messages are delivered to the appliance, it automatically decrypts inbound messages and delivers them to enterprise recipients in the clear. In that way, the encryption of private information is "transparent" to the enterprise users behind the firewall. Intended recipients may not even realize that the information was automatically protected from malicious eyes as it traveled across the internet.

For example, our *ZixGateway*SM users experience simple, automatic and totally transparent email encryption when exchanging secure information with other *ZixGateway* customers. Consumers and other recipients receive via the *Best Method of Delivery*SM either an encrypted *ZixDirect*[®] email or an open email directing them to retrieve an encrypted *ZixPort*[®] message from our secure *ZixMessageCenter*SM.



Automated Inspection of Inbound Email

An electronic appliance can scan incoming email to identify message content and attachments that should have been encrypted by external senders for privacy law or policy compliance, but that were not encrypted and potentially expose private information to a data breach. By identifying these policy lapses, an organization using automated inspection of inbound email can address the attendant privacy and security issues with the external senders.

An electronic appliance uses the enterprise's compliance lexicon to examine the inbound messages in the same way an appliance is used for policy-driven encrypted outbound email. If unprotected private information is detected, the appliance notifies the appropriate internal compliance and data security managers and provides reports logging the details of inbound vulnerabilities, so managers can take appropriate action with senders of unprotected email. For example, our *ZixGateway* Inbound service can help an enterprise ensure that its business associates are taking appropriate steps to protect private information.

Secure Messaging Directory in the Cloud

Conventional email encryption solutions can be difficult to implement and maintain because they require the sender to manage encryption keys for each recipient organization or user. By enabling a shared directory "in the cloud" senders don't have to create and manage encryption keys for each individual or organization with which they communicate. For example, our *ZixDirectory*[™] connects more than 21 million members to enable secure communication among communities of interest, including healthcare, financial services and government. Users can transparently send and receive encrypted emails without having to manage public encryption keys or exchange certificates. By providing customers with an automated directory service in the cloud, solutions such as *ZixDirectory* greatly reduce the typical cost and complexity associated with email encryption solutions.

Conclusion

Electronic commerce relies greatly on email. Email is a principle consumer and business use of the Internet. Email is frequently used to transmit details of online memberships, subscriptions and transactions. The content of email can expose fundamentally private information about consumers, including purchases and website memberships. Consumers must be able to trust that their personal information associated with their email address, as well as personal information transmitted via email, remains secure. Automated encryption of email provides an effective, simple means of protecting personal information and enhancing consumer privacy. The use of automated email encryption technology should be encouraged by governments to enable electronic commerce while simultaneously protecting consumer privacy.

Respectfully submitted,



James F. Brashear
General Counsel
Zix Corporation