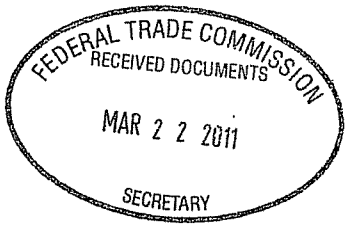
DuaneMorris®

GLENN B. MANISHIN
DIRECT DIAL: 202.776.7813
PERSONAL FAX: 202.478.2875
E-MAIL: gbmanishin@duanemorris.com

www.duanemorris.com

ORIGINAL



March 11, 2011

Donald S. Clark, Secretary
Federal Trade Commission
Office of the Secretary
Room H-113 (Annex W)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* File No. P095416

Dear Mr. Clark:

I enclose for late-filing in the captioned privacy proceeding the comments of Zix Corporation. Zix was unable to prepare and submit its comments by the February 18, 2011 deadline and the Commission's Web-interface for electronic submission is now closed.

We therefore ask that the Commission accept these comments for inclusion as part of its record on the Preliminary FTC Staff Report, and respectfully suggest that permitting late filing is consistent with the Commission's commitment to "encourage full participation by all stakeholders." *See* http://ftc.gov/opa/2011/01/privacyreport.shtm.

Please do not hesitate to contact the undersigned if you or the Bureau of Competition staff have any questions or concerns in this regard.

Thank you in advance for your cooperation.

Sincerely,

Glenn B. Manishin

Encl.
cc: James F. Brashear, Esq., Zix

Before the
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers	)))	File No. P095416

COMMENTS OF ZIX CORPORATION

James F. Brashear
Vice President, General Counsel & Secretary
ZIX CORPORATION
2711 North Haskell Avenue, Suite 2200
Dallas, TX 75204
(214) 370-2219
jbrashear@zixcorp.com

Glenn B. Manishin
DUANE MORRIS LLP
505 9th Street, N.W.
Suite 1000
Washington, DC 20004
(202) 776-7813
gbmanishin@duanemorris.com

Attorneys for Zix Corporation

Dated: March 11, 2011

Before the
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION

Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers	)))	File No. P095416

COMMENTS OF ZIX CORPORATION

Zix Corporation (Zix), by its attorneys, respectfully submits these comments in response to the preliminary staff report (Report) — released Dec. 2, 2010 by the Bureau of Consumer Protection of the Federal Trade Commission (Commission) — on *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers.*[1]

INTRODUCTION AND SUMMARY

The Report proposes a "normative framework" for how private industry "should protect consumers' privacy,"[2] including a controversial "Do Not Track" proposal for online behavioral advertising.[3] In part, the Report "proposes that stakeholders undertake a broad effort to educate consumers about commercial data practices and the choices available to them."[4]

Zix Corporation (Zix) supports this vital education initiative. There can be no doubt that electronic communications, Web-enabled e-commerce and the accelerating substitution of electronic mail (email) for legacy forms of communication are driving the United States' and global economies to an unprecedented level of business efficiency as well as personal and

---

1 Available at http://ftc.gov/opa/2011/01/privacyreport.shtm. On Jan. 21, 20111, the Commission extended the deadline for public comment on the preliminary staff report until Feb. 18, 2011 to "encourage full participation by all stakeholders." *See* http://ftc.gov/opa/2011/01/privacyreport.shtm. Zix was unable to prepare and submit its comments by that date and asks that the Commission accept these late-filed comments for inclusion as part of its record.

2 Report at i.

3 *Id.* at vii.

4 *Id.*

community connectivity. Safeguarding and strengthening the privacy protections governing Internet-based communications and transactions, as well as digital information collected and communicated about offline transactions, is essential to provide the security required by businesses and consumers in order to continue the remarkable growth of this revolutionary medium.

Zix Corporation is the market leader of email encryption services. We provide secure email services to more than 1,200 hospitals and 1,500 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.

Our comments on the Report[5] focus on Zix's area of expertise, in part because the Report is more targeted to Web-site privacy policies, enhancing transparency in data protection practices and catalyzing the development of Fair Information Privacy Practices (FIPPs). What is missing, we believe, is the appropriate and important role of government as an evangelist for consumer Internet privacy. The misalignment of consumer expectations and lack of informed consent highlighted by the Report[6] can also be ameliorated by affirmative outreach programs, with the government as a neutral observer and advocate, which assist businesses and consumers in protecting the privacy of their day-to-day Internet activities and transactions. Since email continues to represent the "killer app" of the Internet economy — the single application employed most by a dominant majority of Internet users — ensuring that email privacy

---

[5] Zix also commented on the Commerce Department's related Notice of Inquiry, *Information Privacy and Innovation in the Internet Economy,* 75 Fed. Reg. 21226 (Apr. 23, 2010), http:// www.ntia.doc.gov/frnotices/2010/ FR_PrivacyNOI_04232010.pdf. Those comments are attached for the convenience of the Commission's staff.

[6] *E.g.,* Report at 25.

expectations are maintained, in the real world, represents an important aspect of Internet privacy which the Report unfortunately understates.

DISCUSSION

The Report's basic conclusion is something with which every enterprise, organization and consumer participating in the Internet ecosystem can and should agree.

> In today's digital economy, consumer information is more important than ever. Companies are using this information in innovative ways to provide consumers with new and better products and services. Although many of these companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner. And while recent announcements of privacy innovations by a range of companies are encouraging, many companies — both online and offline — do not adequately address consumer privacy interests.

Report at i. Yet these concerns are principally directed at the interaction of Internet users with commercial Web sites, whether social networking, e-commerce or otherwise. The Report apparently consider email services — predominately provided by Interest Service Providers (ISPs) and Web-based or "cloud" email services — as an afterthought, if at all. To the contrary, however, the reality is that email has developed into, and remains, the major medium by which electronic communications on the Internet are conducted, including to provide confirmation of the details of many e-commerce transactions.

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 smartphones. 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 near-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.

Obviously, the Report's recommendations for enhanced privacy disclosures and "privacy by design" have applicability to ISPs and other email providers as well as commercial Web enterprises. The principles advocated for purpose specifications, use limitations and accountability are as applicable to email to as ordinary Web transactions. Yet email is in some respects a special case. Although most consumers ordinarily believe email is private, the reality is otherwise. Email is more like a postcard than a letter. Email's content is visible to all who handle the communication. 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. *Rehberg v. Paulk,* 598 F.3d 1268 (11th Cir. 2010). More recently, California's appellate courts decided that even attorney-client privileged emails are not protected if sent from an employer's information technology (IT) system under a corporate policy prohibiting personal use of computers and other IT assets.[7]

---

[7] *Holmes v. Petrovich Development Co.,* ___ Cal. Rptr. 3d ___, 2011 WL 117230 (Cal. App. 3d Dist., Jan. 13, 2011), available at http://www.courtinfo.ca.gov/opinions/documents/C059133.PDF. The court concluded that by using the company's computers to communicate with her lawyer, "knowing the communications violated company computer policy and could be discovered by her employer due to company monitoring of e-mail usage," the employee was not engaged in a confidential electronic discussion with counsel. *Id.,* slip op. at 3. There are different Fourth Amendment issues applicable to whether the government can obtain a suspect's email from his or her ISPs without a warrant, which presents constitutional privacy considerations.

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. Many Web sites require that individuals register using their email address — and that address often becomes the user's log-in identity. An individual's primary email address thus becomes the user's de facto common identity across the Internet, and is considered by most users to be personally identifiable, private information. An individual's email account is a portal into the intimate details of that person's lifestyle. The content of email, individually or in the aggregate, can expose fundamentally private information about people.

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 email providers 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 Web site subscriptions, etc. Moreover, the notion of informed consent presumes that consumers actually understand how data service providers utilize and repurpose 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.

Encryption can make the contents of every email, both the message text and 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 Department of Commerce's 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 person intercepts a copy of an encrypted email while it is moving across the Internet or while it is stored in message archives, that 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. The HIPAA security rule requires that health care providers encrypt electronic protected health information and use encryption or other technologies to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." *See* 45 CFR §§ 164.312(a)(2)(iv), (e)(2)(ii). And a recent Massachusetts regulation requires that any company which "owns or licenses personal information about a resident" of that state must ensure 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."[8]

Zix is one of a number of secure, encrypted email providers in the United State and globally. Unlike the legacy private key infrastructure (PKI) technology introduced in the 1990s, however, Zix's "policy-based" encryption technology does not depend on the initiative of users

[8] 201 C.M.R. § 17.04(3).

to encrypt specific messages and the sometimes incomprehensible technical details of PKI encryption, which requires public and private "keys," the former disseminated to all potential email recipients. All outbound email messages from an enterprise deploying Zix's secured email servers are encrypted automatically without user interaction. While we believe our encryption solution is best-of-breed, Zix is not participating in this proceeding to sell our products. We firmly believe that a public policy focus on email privacy will "lift all boats" and are confident that Zix's encrypted email servers — which allow recipients who do not own our software nonetheless to receive and read encrypted email messages — can and will prevail in the competitive marketplace.

This leads necessarily to our policy proposal. There are statutory requirements, for instance under the Gramm-Leach-Bliley Act and HIPAA, that require companies in sensitive industries to protect the security of patient/customer information, for which encrypted email is an effective and low-cost solution. While we are not so presumptuous to suggest that email encryption should be mandated by the federal government for securities, healthcare or other industries, it remains true that Internet users have developed an exaggerated (and incorrect) sense of trust in the privacy of their email communications. Email can and often is intercepted, hacked, archived and stored on numerous Internet servers without the knowledge or consent of the ender or recipient. The reality is that email users routinely and inaccurately discount the likelihood of interception — malicious or otherwise — and assume their email communications are inherently private.

Zix suggests, therefore, that the federal government should utilize its "bully pulpit" to jump-start consumer adoption of encrypted email as the preferred, self-help remedy for protecting the privacy of Internet email communications. This is hardly an officious suggestion.

This Commission, the federal government's acknowledged leader in privacy, has developed and published a variety of consumer FAQs and advisories on Internet privacy issues.[9] Likewise, the Federal Communications Commission has for years distributed advisories on telemarketing company practices, "VoIP" and other consumer protection issues.[10]

Correcting the misapprehension that email communications are secure and private — whether from interception, malicious hackers or the government itself — is a unique and proper role for government. We believe it is incontestable that the killer app of the Internet, email, will and may be undermined by a lack of public confidence in privacy and security. Such a development would threaten the entire technological edifice on which today's Internet economy has been built. Zix therefore urges the Commission to initiate a consumer education and outreach campaign to inform Internet users that their privacy expectations for email may be misplaced, and that secure, encrypted email represents a simple, technologically proven method of protecting the privacy of their sensitive email communications.

CONCLUSION

For all these reasons, Zix Corporation believes the Commission should initiate a consumer education program addressing the privacy risks inherent in open, unsecured email communications. Such an initiative would be consistent with the consumer protection outreach practices the FTC has historically adopted in the privacy arena and would appreciably add to the

---

9 *See* Report at 13-14.

10 *See* FCC Consumer Advisory, *VoIP and 911 Service,* http://www.fcc.gov/cgb/consumerfacts/voip911.html (Feb. 1, 2011); FCC Consumer Factsheet, *Unwanted Telephone Marketing Calls,* http://www.fcc.gov/cgb/consumerfacts/tcpa.html (Oct. 20, 2008); FCC Consumer Advisory, *The Truth About Wireless Phones and the National Do-Not-Call List,* http://www.fcc.gov/cgb/consumerfacts/ truthaboutcellphones.html (Oct. 16, 2008).

variety of tools available to Internet users to protect the privacy of their personal information and communications in today's electronically connected, always on society.

Respectfully submitted,

James F. Brashear
Vice President, General Counsel &
Secretary
ZIX CORPORATION
2711 North Haskell Avenue, Suite 2200
Dallas, TX 75204
(214) 370-2219
jbrashear@zixcorp.com

By:
Glenn B. Manishin
DUANE MORRIS LLP
505 9th Street, N.W.
Suite 1000
Washington, DC 20004
(202) 776-7813
gbmanishin@duanemorris.com

Attorneys for Zix Corporation

Dated: March 11, 2011

zixcorp

June 4, 2010

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 o f 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 indentify 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.

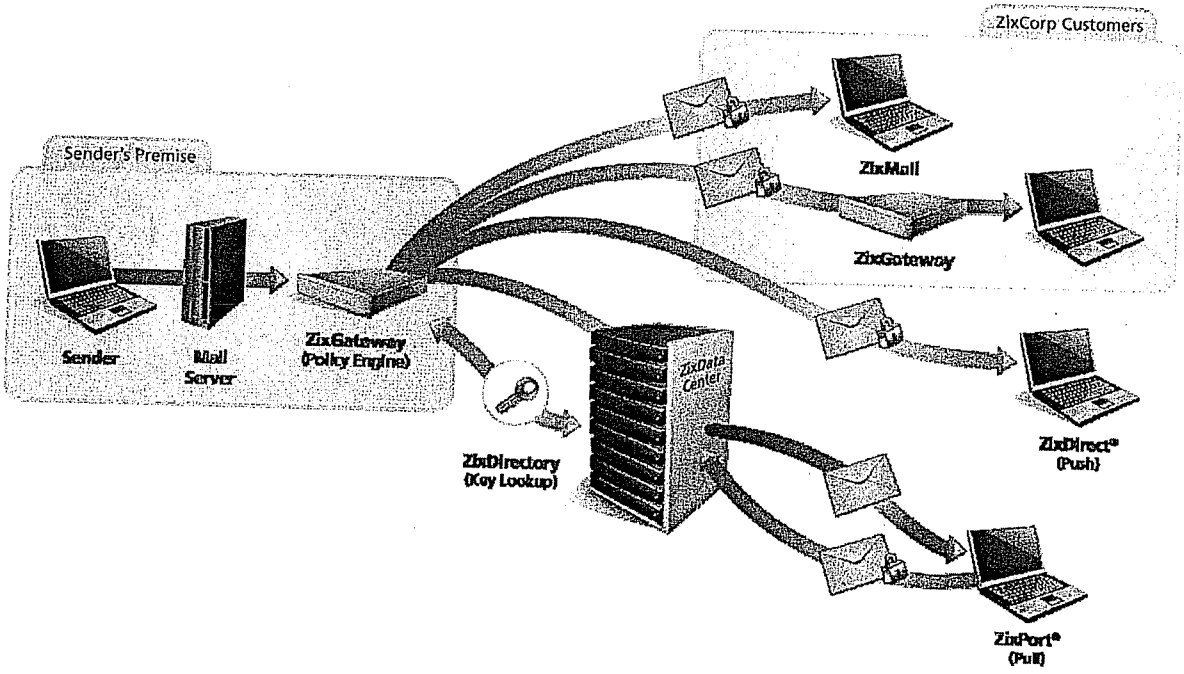
Automated, policy-driven email encryption offers a privacy solution that facilitates compliance with national and state privacy regulations as well as voluntary enterprise practices. An enterprise can adopt a "policy" that prescribes what email must be encrypted based on content, attachments, email address 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*℠ 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*℠ either an encrypted *ZixDirect*® email or an open email directing them to retrieve an encrypted *ZixPort*® message from our secure *ZixMessageCenter*℠.



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