**Before the**
**UNITED STATES DEPARTMENT OF COMMERCE**
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

| | | |
|---|---|---|
| Cybersecurity, Innovation and the Internet Economy | ) | Docket No. 110527305-1303-2 |

# 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: August 1, 2011

**Before the**
**UNITED STATES DEPARTMENT OF COMMERCE**
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

| | | |
|---|---|---|
| Cybersecurity, Innovation and the Internet Economy | ) ) ) | Docket No. 110527305-1303-2 |

## COMMENTS OF ZIX CORPORATION

Zix Corporation (ZixCorp), by its attorneys, respectfully submits these comments on the June 2011 report entitled "Cybersecurity, Innovation and the Internet Economy" by the Department's Internet Policy Task Force (the *Report* or Green Paper).[1] Our comments focus in particular on the series of questions set out in the subsequent Notice and Request for Public Comment[2] regarding development of cybersecurity policies and their impact on the pace of innovation in the Internet and information innovation sector (I3S) of the United States' and global economies.

## INTRODUCTION AND SUMMARY

Secretary Locke's introduction to the *Report* properly acknowledges that the U.S. government for years "has supported the private sector in creating the foundation for the Internet's success."[3] That powerful driver of economic growth and opportunity, however, is threatened by an increasingly dangerous level of cybersecurity intrusions, breaches, worms, malware and related information technology (IT) security hazards. The *Report* therefore recommends that "the

---

1 *Available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908648/.

2 *Notice and Request For Public Comment,* Cybersecurity, Innovation and the Internet Economy, 76 Fed. Reg. 34965 (June 15, 2011) (*Notice*). The *Notice* provides that the Department will accept comments on the issues identified for discussion through Aug. 1, 2011.

3 *Report* at ii.

government and stakeholders come together to promote security standards," and proposes that federal agencies "continue to support both innovations in security and on the Internet more broadly."[4]

ZixCorp supports the Department's timely initiative. ZixCorp is the market leader of electronic mail (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. ZixCorp is thus a visible example of "the American companies that have led the way at every stage of the Internet revolution, from web browsing and e-commerce technology to search and social networking."[5]

Electronic communications, Web-enabled e-commerce and the accelerating substitution of email for legacy forms of communication are leading the United States economy to unprecedented levels of business efficiency as well as personal and community connectivity. Safeguarding the privacy of Internet-based communications and transactions is essential to provide the security and confidence required by businesses and consumers in order to continue the remarkable growth of this revolutionary medium. Because email continues to be the "killer app" of the Internet economy — the single application most-employed by a dominant majority of Internet users — ensuring the security and privacy of email communications is essential to the continued vitality of e-commerce.

---

4 *Id.* at iii.

5 *Id.* at ii.

ZixCorp agrees that more needs to be done to educate, incent and catalyze investment in and attention to cybersecurity and its necessary corollary, online privacy. As the *Notice* summarizes:

> Despite increasing awareness of the associated risks, broad swaths of the economy and individual actors, ranging from consumers to large businesses, do not take advantage of available technology and processes to secure their systems, and protective measures are not evolving as quickly as the threats. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate levels and poses a threat to national security.

*Notice.* 76 Fed. Reg. at 35965. Part of this effort can and should come from the private sector through the development of industry-specific, voluntary norms and best practices for IT security. Part of it, however, needs to come as well from government, which is in a unique position to educate Americans — particularly consumers and small businesses — on both the threats facing online activities and the range of solutions already available for eliminating and curing them. The federal government's "bully pulpit" is particularly suited to such outreach, the social and economic benefits of which would vastly exceed the *de minimis* costs involved.

## DISCUSSION

The broad scope of the *Report,* including its ambitious attempt to define the boundaries of the burgeoning I3S sector of the American economy, presents challenges, such as the likelihood that improved cybersecurity standards and practices for some products and services may and should vary from those applicable to others. The procedural recommendations set forth in the *Report* are principally directed at two quite different risks, namely (i) physical system intrusions, *i.e.*, hacking, and (ii) vulnerability of data exchanged via e-commerce and digital content services, *i.e.,* the interaction of Internet users with commercial Web sites. The Task Force apparently consider email services — predominately provided by Internet Service Providers (ISPs) and Web-based or "cloud" email services — as an afterthought, if at all. To the

contrary, the reality is that email has developed into, and remains, the major medium by which electronic communications on the Internet are conducted.

**A. The Ubiquity of Email**

Access to the Internet is nearly universal in the U.S., and it is increasingly available to consumers using mobile devices. Email is the most prevalent and significant Internet communication technology, and therefore deserves special attention. 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. Email is the main content type accessed by 44% of mobile Internet subscribers via their smartphones. For consumers who do not own a computer, email can be retrieved via an Internet browser using a shared computer, smartphone or tablet. Consumers can access email virtually anywhere — at work, home, school and while traveling — including on airplanes, trains and via WiFi in an increasing majority of public buildings.

Email is extraordinarily simple to use, ubiquitous and flexible. There are a variety of email applications for desktop, laptop and mobile devices. 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. Senders can confirm whether email was delivered and opened. For all these reasons, email has become an integral part of electronic commerce and is the primary method that businesses and individuals use to exchange information.[6] *See, e.g.*, Z. Lasker, *Even In A Social World, Email Is*

[6] Popular media suggests that the ubiquity of email on wireless devices has led to a sort of smartphone compulsion or "addiction" that may be psychologically isolating. S. Murphy, *Addicted To Checking Your Smartphone?*, MSNBC.com, July 25, 2011, *available at* http://www.msnbc.msn.com/id/43884289/ns/technology_and_science-wireless/; E. Barker, *Is Email the New Symbol of Overload In Our Culture?*, BusinessInsider, July 23, 2011, *available at*

*Still The Killer App*, MarketShare, Forbes.com, July 27, 2011, *available at* http://blogs.forbes.com/marketshare/2011/07/27/even-in-a-social-world-email-is-still-the-killer-app ("In recent times, it is email that has driven the growth of the so-called Web 2.0 companies. Be it Groupon, LivingSocial or Pandora, or even any of the social networks, the companies that are the most successful today are the ones that have large and active email user bases.").

**B. Consumer Misperceptions of Email Privacy**

There is a fundamental distinction between email and the even more disruptive communication tools recently popularized by social media. On one hand, most consumers have at least a rudimentary understanding that communications made on Facebook, Twitter or other social networks may not be private or secure and are subject to voluntary privacy policies. On the other hand, consumers generally believe that email is inherently private. The reality is otherwise.

Email is more like a postcard than a sealed 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] Thus, the content of an email is not inherently private.

---

http://www.businessinsider.com/is-email-the-new-symbol-of-overload-in-our-culture-2011-7. The social consequences of an always-connected citizenry is an issue quite different from IT security, but underscores that the portion of activities conducted online today is growing in both scale and importance.

[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

Furthermore, an individual's email address and account 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.

**C. Privacy and Security Issues in Email**

There are a variety of privacy and security issues raised by the omnipresent use of email that should be reflected in the Department's response to the Task Force recommendations. In addition to the general privacy issues noted above, the vulnerability of email to hacking, snooping, phishing and related digital scams seriously compromises the basic privacy of electronic correspondence, potentially threatening the economic viability of email as a commercial communications medium.

Although it is possible for a consumer to "opt out" by changing to an email provider whose security and privacy policies are more protective of individual rights, it is impractical for

---

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.

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 ISPs and 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. As we discuss below, technology also supports the type of "automated security" for email that falls within the sweet spot of the areas on which additional comment has been requested. *See Notice,* 76 Fed. Reg. at 34966 (questions 18 through 21).

**D. Privacy Protection in Encrypted Email**

One way of ensuring the security and privacy of email communications is to encrypt the content. Encryption can make the substance of every email, both 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'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.

Unlike the legacy private key infrastructure (PKI) technology introduced in the 1990s, however, ZixCorp's "policy-based" encryption technology does not depend on the initiative of users to encrypt specific messages, nor do users need to fathom the incomprehensible technical details of PKI encryption, which requires public and private "keys," the former disseminated to

all potential email recipients. The encryption process can be virtually transparent to both senders and receivers.

All email messages (subject, text and attachments) outbound from an enterprise deploying ZixCorp's ZixGateway® secured email servers are scanned and are encrypted automatically if they contain confidential content. This is a simple technological fix to the security vulnerability of requiring humans to determine if a message should be encrypted and remembering to encrypt it before clicking "Send." If the recipient has not subscribed to ZixCorp's services, our encrypted email portals — which can be branded by the sending organization — allow any recipient to read encrypted email delivered via our services and reply securely, without charge. Our newest mobility solutions support the secure delivery of policy encrypted email to smartphones and tablet devices as well.

Similar automated scanning and encryption processes can be applied to emails that are generated by computers, as opposed to emails drafted by humans. We refer to these automatically-generated emails as being "application driven." They can be compared to automatically-generated form letters, but are sent electronically rather than via post. When automatic scanning and encryption is applied to these emails, we refer to the process as Application Generated Encrypted Email (AGEE). We currently provide AGEE services to a federal banking regulator when it sends to member institutions automatically-generated periodic reports. AGEE may be a particularly important cybersecurity practice for specific industries, such as health care and financial services, in which existing legal standards impose an informational security obligation on private firms.

## E. Regulatory Precedent And Incentives

The U.S. government and state governments have acknowledged that encryption of email is an effective means of protecting confidential information. There are outstanding federal laws that today require companies in a few, especially sensitive economic sectors to protect the integrity and privacy of consumer information. For instance, financial information is protected by the Gramm-Leach-Bliley Act and personal health information is protected under HIPAA.[8] Similarly, 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."[9]

---

[8] The final HIPAA Security Rule makes use of encryption for open network communications a so-called "addressable implementation specification." 45 C.F.R. §§ 164.312(a)(2)(iv) and 164.312(e)(2)(ii). Under this approach, encryption must be implemented if a covered health care entity determines that the specification is appropriate in its environment, while documenting any contrary determination and applying an equivalent alternative security measure. Under the GLB Act, the Federal Trade Commission's Safeguards Rule requires financial institutions subject to its jurisdiction to have measures in place to keep customer information secure; the FTC recommends consideration of encryption of electronic customer information while in transit or in storage. *See* FTC, Financial Institutions and Customer Information: Complying with the Safeguards Rule, *available at* http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule. The interagency Federal Financial Institutions Examination Council (FFIEC) is more explicit: "Financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit." *See* FFIEC Handbook, *available at* http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/encryption.aspx. Likewise, the PCI Data Security Standard (PCI DSS) for credit card processing, *available at* http://www.pcisecuritystandards.org/security_standards, includes a requirement that "[s]ensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit."

[9] 201 C.M.R. § 17.04(3). Nevada has enacted an almost identical statutory requirement. Nevada Rev. Stat. § 597.970 (prohibiting "a business in this State" from transferring outside of its secure system "any personal information of a customer through an electronic transmission," except via facsimile, "unless the business uses encryption to ensure the security of electronic transmission").

While we are not so presumptuous to propose that email encryption should be mandated by the government for ordinary commercial transactions, it remains true that Internet users have developed an exaggerated (and incorrect) sense of trust in the privacy of their email communications.[10] ZixCorp suggests, therefore, that the Department consider legal, policy and outreach changes to incentivize the more general adoption of email encryption. These measures could include, for example, (a) structuring liability standards for IT security breaches as a sliding scale, under which services offered with automated, technical security protections (such as AGEE encryption) would be subject to less rigorous legal scrutiny, lower monetary damages, or both (*see Report* at 23-24), and (b) requiring disclosure of security practices, much as the government's groundbreaking efforts have within just more than a decade led to the near-ubiquitous, voluntary adoption and disclosure of Web-site privacy policies (*see Report* at 27-29).[11] The latter would be a particularly useful practice if applied to ISPs and email hosting companies, as an array of relatively simple precautions (such as logging on via a secure SSL, or "https," connection and periodic prompting for password changes) are also available. Encouraging competition among commercial email providers not only on visible product factors such as

---

[10] Email can and often is intercepted, hacked, archived and stored on numerous Internet servers without the knowledge or consent of the ender or recipient. *See, e.g., Google Reveals Gmail Hacking, Says Likely From China,* Reuters, June 2, 2011, available at *http://www.reuters.com/article/2011/06/02/us-google-hacking-idUSTRE7506U320110602.* The unfortunate reality, however, is that email users routinely and inaccurately discount the likelihood of interception — malicious or otherwise — and assume their email communications are inherently private. Although the Report addresses emerging technologies for sender-identification in email and DNS security, *Report* at 16, 35, 61-64, such measure ameliorate risks from spam and "phishing," not from the interception of email content.

[11] There is a wide range of legal areas in which security can be enhanced without mandating specific technologies or practices. For instance, pharmaceutical refill reminders, overdraft notices and the like could all benefit from the vastly increased security of email encryption to satisfy existing legal obligations. For industries not subject to information security mandates, the liability safe harbor suggested above in the text of these comments would be preferable, in some ways, as it could be applied uniformly in a variety of different e-commerce markets, encouraging uniform application of email security without unnecessary technological intrusiveness.

storage capacity and price, but also on privacy and security, would protect consumers while allowing the marketplace itself to align customer expectations with email product development. We agree that the Department should strive to "increase the security posture of I3S services and functions from cybersecurity risks without regulating these services as covered critical infrastructure." *Report* at 3.

Finally, 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. *See Report* at 35-38. This is hardly an officious suggestion. The FTC, the government's acknowledged leader in privacy, has developed and published a variety of consumer FAQs and advisories on Internet privacy issues. Likewise, the Federal Communications Commission has for years distributed advisories on telephone companies billing practices, "slamming" and other consumer protection issues.

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 Department 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.

We believe such an approach would balance the legitimate interests of all stakeholders, and protect digital security and privacy without discouraging businesses and consumers from

continuing to take advantage of the efficiencies of modern communication technologies. ZixCorp is one of many secure, encrypted email providers in the United State and globally. We are convinced our products are best-of-breed, but ZixCorp is not participating in this proceeding to sell services. A public policy focus on email security is in the public interest and meets a pressing need with respect to consumer privacy; ZixCorp believes that from a competitive perspective, our automated technological solutions for protecting email security can and will prevail in the marketplace.

## CONCLUSION

For these reasons, ZixCorp proposes that the Department consider requiring disclosure of cybersecurity practices by e-commerce companies, especially ISPs and firms interfacing directly with consumers, and initiate a consumer education program addressing the security and privacy risks inherent in open, unsecured email communications. Such an initiative would be consistent with the consumer protection practices of other federal government agencies and would appreciably add to the variety of tools available to Internet users to protect the security 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: Aug. 1, 2011