Before the
UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct	)	Docket No. 120214135-2135-01 RIN 0660-XA27

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 30, 2012

Before the
UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct	)))	Docket No. 120214135-2135-01 RIN 0660-XA27

COMMENTS OF ZIX CORPORATION

Zix Corporation (ZixCorp), by its attorneys, respectfully submits this response to the National Telecommunications and Information Administration's ("NTIA" or the "Department") request for comment[1] on the February 2012 White House report, CONSUMER DATA PRIVACY IN A CONNECTED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (the "*Privacy and Innovation Blueprint*").[2]

DISCUSSION

The *Privacy and Innovation Blueprint* articulates for the first time in America a so-called Consumer Privacy Bill of Rights. It further proposes that the federal government, through NTIA, convene and supervise a voluntary process — within specific industry sectors — for exploration and adoption of codes of conduct relative to consumer privacy and data security. Enforcement of

[1] Request For Public Comment, *Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct,* 77 Fed. Reg. 13.098 (March 5, 2012) ("RFC" or "Request"). NTIA has extended the deadline for response to the RFC to April 2, 2012.

[2] Hereafter the ''Privacy and Innovation Blueprint," a*vailable at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Blueprint builds on the recommendations of the Department of Commerce Internet Policy Task Force's report, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (Dec. 2010) (*available at* http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework.), a public comment process in which ZixCorp also participated.

these voluntary codes would be by the Federal Trade Commission ("FTC") under its consumer protection authority.

Among other things, the present RFC asks for input on what data privacy issues should be addressed in this multistakeholder process for code of conduct development, such as mobile device privacy notices, cloud computing services, trusted identity systems and teenage/child protection. ZixCorp[3] suggests that an important issue to be considered in the voluntary data privacy codes is implementation of the Security principle of the Consumer Privacy Bill of Rights.

Security: Consumers have a right to secure and responsible handling of personal data.

Privacy and Innovation Blueprint at 1, 19.

Consumer data security is not achieved merely through deployment of technical firewalls and safeguards against deliberate IT network intrusions; it also implicates protection of digital information privacy during its electronic transmission among companies, their customers and corporate partners and vendors. Privacy thus requires that (a) consumers be educated about the risks associated with sending personally identifiable information ("PII") on unsecured WiFi networks through open Internet protocols, such as POP email, that offer no data protection at all, and (b) companies be incentivized to move customers away from the unfortunately ubiquitous

[3] 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." U.S. Department of Commerce, Internet Policy Task Force, CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY at ii (June 2011), *available at* http://www.nist.gov/customcf/ get_pdf.cfm?pub_id=908648/.

practice of utilizing email addresses, which are readily harvested and sold, as a form of digital identity management.

A. Consumer Data Privacy Is Inextricably Linked To Data Security

It goes almost without saying that "[m]uch of the personal data used on the Internet . . . is not subject to comprehensive Federal statutory protection, because most Federal data privacy statutes apply only to specific sectors, such as healthcare, education, communications and financial services or, in the case of online data collection, to children." *Privacy and Innovation Blueprint* at 6. Likewise apparent, although less well known to the general public, is that "consumers have certain responsibilities to protect their privacy as they engage in an increasingly networked society." *Id.* at 9.

Privacy without data protection is meaningless. Unfortunately, many Internet end users have developed an exaggerated sense of privacy with respect to routine Web-based transactions that professionals know all too well can and are being archived, stored and mined by a variety of commercial enterprises. Safeguarding the privacy of Internet-based communications and transactions is thus essential to provide the confidence required by businesses and consumers in order to continue the remarkable growth of the Internet ecosystem. Because email remains the "killer app" of the Internet economy — the single application most-employed by a dominant majority of Internet users[4] — ensuring the security and privacy of email communications is essential to the continued vitality of e-commerce.

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 an explanation of

[4] 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.

the Consumer Privacy Bill of Rights' Security principle, it is difficult to disagree that "[c]omp-anies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure." *Privacy and Innovation Blueprint*\ at 19. But as an earlier *Notice* emphasized:

> 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 and Request For Public Comment, *Cybersecurity, Innovation and the Internet Economy,* 76 Fed. Reg. 34965, 35965 (2011).

This suggests that the Security principle most assuredly deserves to be included among the topics for multistakeholder "best practices" development. Yet it also clearly necessitates that government agencies, corporations and consumer advocates all collectively resolve to educate Americans — particularly end users and small businesses — on the security threats facing online activity 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.

B. <u>The Security Principle Should Be Expanded To Encompass Electronic Communications Among Companies, Customers And Commercial Third-Parties, With A "Safe Harbor" Preference For Encryption</u>

"Responsible" handling of consumer data of course calls for an increase in resources applied to IT security within consumer-facing companies, whether those providing technology products and services or traditional consumer merchandise retailers. The many state data breach notification laws, as well as pending congressional legislation on cybersecurity that would

extend breach notice requirements nationwide, have begun to encourage holders of consumer PII to ramp up attention to network and data security in order to minimize their potential legal exposure for unauthorized intrusions.

A useful provision in many of these legislative actions can serve as the model for a Security principle code of conduct. Where a corporation holding PII communicates such information electronically to a customer, vendor or third-party, these cybersecurity bills generally presume that the company has taken reasonable steps for data protection if it applies encryption or some other equivalent technology to preventing misuse of transmitted data. That is, encryption of email and other electronic communications is not mandated, but instead the burden shifts to an alleged victim if data whose security may have been compromised was rendered technically unreadable by others.[5]

This would be an extraordinarily helpful element of a data security code of conduct. The status of the Internet as a powerful driver of economic growth and opportunity is threatened today by an increasingly dangerous level of cybersecurity intrusions, breaches, worms, malware and related IT security hazards. In this context, it is relevant to differentiate two 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. 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*

[5] Of the principal cybersecurity bills presently under consideration by Congress (S.1511 (Leahy), S.1207 (Pryor), S.1408 (Feinstein), S.1434 (Carper), H.R. 1841 (Stearns). H.R. 1707 (Rush). H.R. 2577 (Bono Mack)), only one does not include a presumption or other safe harbor provision offering comfort to firms utilizing encryption to protect the integrity and security of confidential consumer data during transmission.

[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,

Social World, Email Is 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."). Yet the contents of an email are not inherently private. [7] Consequently, any implementation of the Bill of Rights' Security principle which does not address the security of email communications that transmit sensitive data or legally protected PII will necessarily be too narrow to reflect the real-world risks facing consumer digital privacy in today's marketplace.

Less directly implicated, but perhaps even more important, is that on commercial Web sites consumers' email address are often used as a digital substitute for identity. Consumer emails are highly valuable data because, among other things, they can be associated with what an 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

---

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* 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] 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).

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 email account is essentially a portal into the intimate details of an individual's digital lifestyle. Although it is possible for a consumer to "opt out" by changing to an email provider whose security 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 address to all of their personal and business contacts, update Web site subscriptions, etc. Moreover, the notion of informed consent presumes that consumers actually understand how ISPs and service providers utilize and repurpose the personal data they obtain in providing services, and the implications of how their personal data might be utilized.

As those are high barriers (ones data mining companies have an incentive to understate or obfuscate), a presumption that encrypted email encompasses no appreciable risk to the security of its digital content even if stolen or inadvertently disclosed is a narrow, market-oriented approach to catalyzing attention to email security risks and available market alternatives. For instance, using ZixCorp's commercial servers, all email messages (subject, text and attachments) outbound from an enterprise deploying ZixCorp's ZixGateway® secured email servers are scanned and 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."[8]

[8] This approach may not be necessary where sector-specific privacy regulations already incorporate a preference for encryption. The final HIPAA Security Rule, for instance, makes use of encryption for open network communications a so-called "addressable implementation

Requiring disclosure of security practices — much as the FTC's groundbreaking efforts have within just more than a decade led to the near-ubiquitous, voluntary adoption and disclosure of Web-site privacy policies — would be a particularly useful if applied to ISPs and email hosting companies, because an array of relatively simple precautions (such as logging on via a secure SSL, or "https," connection and periodic prompting for password changes) is also available. Encouraging competition among commercial email providers not only on visible product factors such as 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.

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. This is hardly an officious suggestion. The FTC 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

---

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."

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 proper role for government.[9]

CONCLUSION

NTIA should include the "Security principle" from the *Consumer Privacy Bill of Rights* ("Consumers have a right to secure and responsible handling of personal data") in its development of voluntary codes for data privacy. ZixCorp suggests that requiring disclosure of cybersecurity practices — especially by ISPs and firms interfacing directly with consumers — and initiation of an education program addressing the privacy risks inherent in open email communication would appreciably help protect the security of personal digital information 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: /s/ Glenn B. Manishin
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 30, 2012

[9] 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.