Before the
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION

Debt Collection 2.0: Protecting Consumers As Technologies Change	))	Project No. P114802

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: May 27, 2011

Before the
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION

Debt Collection 2.0: Protecting Consumers As Technologies Change	))	Project No. P114802

COMMENTS OF ZIX CORPORATION

Zix Corporation (ZixCorp), by its attorneys, respectfully submits these comments on the Commission staff's April 28, 2011 public workshop addressing consumer protection issues that have arisen as debt collectors avail themselves of advances in technology. Our comments focus in particular on the series of questions set out in the Commission's accompanying Public Notice[1] regarding use by debt collectors of modern communication technologies, such as electronic mail and social network messaging.

INTRODUCTION AND SUMMARY

The *Notice* correctly observes that, in the decades since enactment of the Fair Debt Collection Practices Act (FDCPA), 15 U.S.C. § 1692 *et seq.,* advances in communication technologies have greatly expanded debt collectors' means and ability to access consumers.[2] This is an especially important matter for public policy and Commission enforcement of the FDCPA because these technological developments "raise potential consumer protection concerns . . . including the security of electronic communications, whether such communications satisfy the

---

1 *Public Notice,* Debt Collection 2.0: Protecting Consumers as Technologies Change, 76 Fed. Reg. 14010 (March 15, 2011) ("*Notice*"). The *Notice* provides that the FTC will accept comments on the issues identified for discussion at the workshop until May 27, 2011.

2 *Notice,* 76 Fed. Reg. at 14011

[statute's] written notice requirements, and how they implicate the FDCPA's prohibition against contacting consumers at inconvenient times or places."[3]

ZixCorp supports the Commission's timely inquiry. 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.

Electronic communications, Web-enabled e-commerce and the accelerating substitution of 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 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.[4] Because email continues to be the "killer app" of the Internet economy — the single application most-employed by a dominant majority of Internet users — safeguarding the security and privacy of email communications is essential to the continued vitality of e-commerce.

Government should act to ensure that the basic United States consumer protection policies and laws, such as the FDCPA, are applied and adapted to meet the challenges posed by the Internet. Although the FTC does not have authority to issue regulations implementing the

---

3 *Id.* at 14012.

4 *See generally* ZixCorp's comments in the Commission's privacy-related proceedings, including the Bureau's Dec. 2010 preliminary staff report, File No. P095416, and our earlier comments 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.

FDCPA, the Commission is empowered to enforce the FDCPA under Section 5 of the FTC Act.[5] We encourage the FTC to take these communications technology concerns into account in its enforcement actions and its legislative recommendations to Congress.

DISCUSSION

No less than other industries, the debt collection business is rapidly being transformed by what the *Notice* terms "post-FDCPA communication technologies."[6] Clarifying the propriety of these new communications practices under the FDCPA, and harmonizing the statute's balance among concerns for accuracy, confidentiality and prevention of consumer harassment, are important, albeit challenging, endeavors. The *Notice* correctly states that "although electronic mail is not a new technology, its use by debt collectors to contact consumers has increased, giving rise to questions about its treatment under the current regulatory scheme."[7]

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

---

5 15 U.S.C. § 45(a).

6 *Notice,* 76 Fed. Reg. at 14011

7 *Id.* at 14011.

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. It is no wonder that debt collectors are using email to communicate with consumers.

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.[8] Thus, the content of an email is not inherently private. Contents of debt collection emails are no different.

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 Issues in Email for Debt Collection

There are a variety of privacy and security issues raised by the use of email for debt collector communications with consumers. In addition to the general privacy issues noted above, the vulnerability of email to hacking, snooping, phishing and related digital scams seriously

---

[8] *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.

compromises the basic privacy of debt collector-consumer communications that the FDCPA assumes by virtue of its "written notice" predicate.[9]

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 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.

D. Privacy Protection in Encrypted Email

One way of ensuring the privacy of debt collection email communications is to encrypt the content. Encryption can make the substance 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

[9] FDCPA §§ 805(c), 809(a), 15 U.S.C. §§ 1692c(c), 1692g(a). The FDCPA defines "communication" broadly as "the conveying of information regarding a debt directly or indirectly to any person through any medium," FDCPA § 803(2), 15 U.S.C. § 1692a(2), which covers email, but does not specifically define "written notice." The only specificity the Act provides regarding communication is when communications may be made, certain required content and, if applicable, to whom the communication may permissibly be directed.

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.

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 Driven Encrypted Email (ADEE). We currently provide ADEE services to a federal banking regulator when it sends to member banks automatically-generated periodic reports.

ADEE distribution may offer a low-cost, secure mode for debt collectors to automatically generate email "form letters" that could be automatically encrypted and sent.[10]

E. Regulatory Precedent

There are some laws that already require companies to protect the security of sensitive consumer information in contexts other than debt collection. For instance, financial information is protected by the Gramm-Leach-Bliley Act and health information is protected under HIPAA. For companies involved in the finance and healthcare industries, encrypted email (including ADEE) is an effective and low-cost compliance and privacy solution.

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 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."[11]

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 communi-

---

[10] The *Notice* inquires about their applicability of other laws to post-FDCPA communications technologies. 76 Fed. Reg. at 14014 (asking how current federal and state laws apply to debt collectors' and consumers' use of post-FDCPA communication technologies). For the most part, the principal such federal laws are the CAN-SPAM Act, the Telephone Consumer Protection Act (TCPA) and the Commission's implementing regulations, including the Telemarketing Sales Rules. For a variety of technical reasons, including but not limited to the fact that debt collector communications either do not fall within the scope of commercial solicitations or are exempted as a form of established business relationship or product fulfillment communication, these other statutes and regulations are largely inapplicable. *See generally* 15 U.S.C. § 7702(2) and 16 C.F.R. § 316 ("commercial electronic mail message"); 47 U.S.C. § 227(a)(4) ("telephone solicitation"); 15 U.S.C. § 6106(4) and 16 C.F.R. § 310.2(dd) ("telemarketing").

[11] 201 C.M.R. § 17.04(3).

cations.[12] ZixCorp suggests, therefore, that the Commission should consider recommending to Congress that, if the FDCPA is updated, email communications be deemed to satisfy the Act's "written notice" requirement provided they are encrypted.[13] The purpose of this statutory predicate to debt collector communications with consumers was to provide a private, formal and clear means for debt collectors to forward certain key information about their legal rights to putative debtors. Although "snail mail" has historically been deemed to meet that written notice requirement, it is less clear whether the same is true for unencrypted email.

To encourage responsible use of email, we propose an FDCPA rule that permits initial "written notice" communications to satisfy the statute's predicates whether they are made via hard copy delivery or encrypted email delivery.[14] We believe such a revision would balance the legitimate interests of all stakeholders, and protect consumer privacy without deterring debt collectors from taking advantage of the efficiencies of modern communication technologies. Under this approach, the initial written notice communication from a debt collector would satisfy FDCPA where made via encrypted email, but later electronic communications could use other technologies. Some of these other, newer technologies — such as SMS messaging (texting) and

---

[12] 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. *See* section B above.

[13] Alternatively, the FDCPA could be revised to provide that prior consumer consent to receive email communications from a debt collector is not required if such communications are encrypted. *See Notice,* 76 Fed. Reg. at 14012 (asking whether debt collectors should be required to obtain consumer consent to use particular methods of communication to contact consumers and, if so, which communication methods and why).

[14] The courts' struggles over harmonizing the FDCPA's provisions with answering machine and voicemail technology are instructive on the need for clarification of the propriety and conditions for email communication by debt collectors. *See, e.g., Foti v. NCO Financial Systems,* 2006 U.S. Dist. LEXIS 13857 (SDNY 2006); *Hosseinzadeh v. M.R.S. Assocs., Inc.,* 387 F. Supp. 2d 1104 (C.D. Cal. 2005); *Joseph v. J.J. Mac Intyre Cos., LLC*, 281 F. Supp. 2d 1156 (N.D. Cal. 2003).

social media DMs (direct messages) — present different issues of privacy, security and formality that make their use under the FDCPA rather problematic. ZixCorp would be pleased to participate in the debate over these other new media but does present itself as an expert in their delivery or use, so they are not addressed in these comments.

ZixCorp is one of a several secure, encrypted email providers in the United State and globally. Although we think our encrypted email solutions are best-of-breed, ZixCorp is not participating in this proceeding to sell our services. We firmly believe that a public policy focus on email privacy is in the public interest, meets a pressing need with respect to consumer privacy and, from a commercial perspective, that our technological solutions for protecting email security can and will prevail in the competitive marketplace.

CONCLUSION

For all these reasons, the Commission should consider recommending to Congress that, if the FDCPA is updated, email communications be deemed to satisfy the Act's "written notice" requirement if they are encrypted. This would represent a timely revision to a landmark but outdated statute that in many ways sets the foundation for consumer rights in the United States.

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: May 27, 2011