



May 30, 2014

VIA ELECTRONIC SUBMISSION

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

Re: *Mobile Security Project, Project No. P145408*

Dear Secretary Clark:

Zix Corporation (ZixCorp) appreciates the opportunity to submit these comments in response to the April 17, 2014 request by the Federal Trade Commission (FTC) for further public reaction to the issues raised at last year's FTC mobile security forum.

The Commission's 2013 forum consisted of a day-long series of panel discussions and presentations addressing an array of security issues in the mobile space, including current and potential threats to user privacy and the efficacy of consumer-facing mobile security products, such as authentication and antivirus products. The FTC's current request is directed more precisely to issues affecting (a) secure platform design, (b) secure distribution channels for mobile applications, (c) secure development practices, and (d) security lifestyle and updates for mobile devices. Many of the specific questions posed by the Commission in its April further request focus on the impact of mobile security to consumers, without differentiating between individuals and enterprises (whether small businesses or large public companies) as mobile service users.

ZixCorp is a leader in email data protection. ZixCorp offers industry-leading email encryption, a unique email Data Loss Prevention (DLP) solution and an innovative email Bring Your Own Device (BYOD) solution to meet data protection and privacy compliance needs. ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government for easy to use secure email solutions.

A rapidly-increasing data security concern for enterprises is the exposure of corporate email and attachment data on mobile devices, particularly as more and more companies adopt BYOD policies. Employees are increasingly using their personally-owned mobile devices to store and send confidential corporate and customer information, where it may be exposed to risks of interception or exposure. Many employers attempt to address the corporate data security concerns by taking a degree of control over their employer's mobile devices – using containerization or mobile device management (MDM) solutions that sacrifice employee privacy.

The FTC's study of mobile security issues would be substantially incomplete if the FTC does not examine the data security risks associated with corporate data (including email) on employees' personally-owned devices and the employee privacy concerns arising from over-reaching employer BYOD policies and technology solutions.

ZixCorp believes the Commission's mobile security efforts should focus not merely on the privacy and security of digital information stored on mobile devices, but also on the exposure of such information when transmitted to and from such devices. We stress this aspect of mobile security because weak or non-existent security measures in the transmission of private and confidential information can just as easily lead to data breaches and improper data disclosure as the loss, theft or malware infection of devices themselves.

In 2012, the Department of Defense (DoD), General Services Administration (GSA) and National Aeronautics and Space Administration (NASA) collectively proposed to amend the Federal Acquisition Regulation so that federal government contractors would be obligated to transmit proprietary government information "using technology and processes that provide the best level of security and privacy available, given facilities, conditions and environment." Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51496, 51499 (Aug. 24, 2012). The Commission should follow the earlier lead of these sister agencies and recommend in its forthcoming report on mobile security, at least as a best practice, that enterprises and individual end users likewise take steps (whether encryption or others, as discussed below) to secure sensitive information when transmitted to/from mobile devices.

Given technological change and evolving user preferences, "transmission" must be evaluated in a context broader than simple electronic mail. There already exist a variety of digital communications technologies that support mobile voice and data communication outside of traditional SMTP, POP or Microsoft Exchange email. These include "chat" and instant messaging services such as Google Chat and Google+ Hangouts, Apple's iMessage, instant messaging services from AOL, Yahoo! and ICQ, and Skype and other audio/video technologies supporting half- or full-duplex real-time voice and video communication. Some of these services, most notably Facebook Messenger, resemble email in that they send electronic messages from and to specifically addressed persons and are ostensibly private. (Like other "free" Web email and advertiser-supported services, however, such messages are mined by the provider for data that is sold to advertisers.) Assessment of mobile device security should therefore be expanded to cover email, text (SMS or MMS) messages, chat, video chat and instant messaging services, social media and digital device messaging services and similar communications.

The benefit of a generic transmission security obligation is that it would presumably apply to any information technology configuration, including not-yet invented IT systems and software or apps that may be developed by consumer-facing Internet firms in the future. Current digital privacy and security standards in fields such as health care (HIPPA) and financial

services (Gramm-Leach-Bliley Act)<sup>1</sup> already create email security requirements that are specific to those industries, but there is no legal or public policy reason to limit email security to a few “silo” markets. Mobile devices are now ubiquitous and, as prominent analyst Mary Meeker noted this week, mobile data traffic is up a remarkable 81%, with rapidly accelerating growth, in part because “mobile devices and sensors are capturing and uploading troves of findable and shareable data.” Mary Meeker: *Mobile Devices Equal Big Data Devices*, InfoWorld, May 29, 2014, at <http://www.infoworld.com/t/mobile-technology/mary-meeker-mobile-devices-equal-big-data-devices-243305>.

Healthcare and financial services are not the only industries in which encryption is mandated, preferred or recommended. The Commission’s own 2011 publication, *Protecting Personal Information—A Guide for Business*, offers advice for the collection and storage of personally identifiable information (PII), including physical and electronic security. The FTC guide specifically counsels businesses handling PII to *encrypt sensitive information* that you send to third parties over public networks (like the Internet) and to consider encrypting email transmissions within your business if they contain personally identifying information. The guide notes that *regular email is not a secure method for sending sensitive data.*<sup>2</sup> In the private standards arena, the PCI Data Security Standard (PCI DSS) for credit card processing<sup>3</sup> 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.* And NIST’s guidelines for enterprise mobile device security stress the need for “strongly encrypt[ed] data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of secure protocols and encryption.” NIST Special Publication 800-124, Rev. 1, at vii, 8 (June 2013).

Indeed, the FTC itself warned three years ago that “despite increasing awareness of the [cybersecurity] 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 [IT] systems, and protective measures are not evolving as quickly as the threats.” Notice and Request for Public Comment, *Cybersecurity, Innovation and the Internet Economy*, 76 Fed. Reg. 34965, 35965 (June 15, 2011). Encryption technologies, which have evolved considerably over the past decade and, like digital compression, are now integrated into many computer operating systems, are widely regarded as one of the

---

<sup>1</sup> The HIPPA security rule treats email encryption as a so-called *addressable implementation specification*, meaning it is the preferred method to satisfy the basic standard of assuring the security of protected health information (PHI) when transmitted over public networks. 45 C.F.R. § 164.312(a)(2)(iv), (e)(2)(ii). Under GLBA, the security standards for customer financial information are established by the Federal Financial Institutions Examination Council (FFIEC), which provides extensive, evolving guidelines for compliance with the statutory mandate that financial institutions maintain the security and privacy of customer information. The recommended FFIEC guidelines make the establishment of security controls which *employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit* a best practice in the financial services industry. FFIEC, *IT Examination Handbook InfoBase*, <http://it handbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/encryption.aspx>.

<sup>2</sup> Available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

<sup>3</sup> Available at [http://www.pcisecuritystandards.org/security\\_standards](http://www.pcisecuritystandards.org/security_standards).

best available means to protect the security of secret or sensitive digital information.<sup>4</sup> Encryption is not a panacea, but it certainly renders the electronic information unreadable and unusable to hackers and other unauthorized recipients in the vast majority of cases not involving sophisticated attacks utilizing supercomputer capabilities to crack encryption algorithms.

Employees now expect to use their personal devices to work remotely how and when they need to. But that convenience runs counter to corporate efforts to protect confidential data and stay privacy compliant. Many enterprises have adopted BYOD policies which rely on mobile device management (MDM), typically the ability to remotely “wipe” data from a lost, stolen or compromised device, as the mechanism for ensuring data security. That, too, is not a sustainable long-term solution, as wiping digital devices destroys personal as well as corporate data and it is relatively trivial for intelligent thieves and hackers to defeat MDM simply by turning off a mobile device, or disabling WiFi and cellular services (e.g., airplane mode), or shielding the device from wireless network connectivity (e.g., using a Faraday bag).

ZixCorp has developed a new product, *ZixOne*<sup>®</sup>, that offers corporations an order of magnitude improvement in BYOD email security by never storing the contents of email messages, or attachments, on employees’ mobile devices. See Simple BYOD Approach to Protect Mobile Data With *ZixOne*, <http://www.zixcorp.com/byod/>. We believe our encryption and BYOD solutions are best-of-breed,<sup>5</sup> but are not so audacious to propose that any specific technology or vendor should be selected, or that email encryption should be mandated for ordinary commercial transactions. On the other hand, the market need for and acceptance of innovative new products such as *ZixOne* demonstrate clearly that mobile security needs to be addressed in the context of enterprises as well as individual end users, since a large and increasing proportion of the latter are today using a single device for both personal and corporate mobile communications.

In conclusion, the FTC’s mobile security review and report should recommend security practices that parallel health information, banking and other existing IT security standards by preferring encryption or other secure transmission methods for mobile email and messaging. This is especially important in today’s emerging era of BYOD, since the opportunities for injury to consumers by theft, loss or disclosure of private information have expanded greatly with the diffusion of PII and other sensitive data far beyond the enterprise firewall. Any examination of mobile security that focuses only on consumer-facing applications to the

---

<sup>4</sup> At the state level, Massachusetts and Nevada have promulgated rules requiring all businesses to encrypt confidential digital information about state citizens before electronic transmission, including via email. 201 C.M.R. § 17.04(3); Nevada Rev. Stat. § 597.970. Encryption was also included in most of the federal cybersecurity bills introduced in the 112th Congress. In legislation such as S. 1511 (Sen. Leahy), H.R. 1841 (Rep. Stearns) and H.R. 2577 (Rep. Bono Mack), data breaches suffered by private companies would presumptively not be reportable to customers if the information was encrypted. Other proposed IT security legislation, such as S. 1207 (Sen. Pryor) and H.R. 1707 (Rep. Rush), would, in addition, require implementing FTC rules to include use of specific technologies for data security, including encryption.

<sup>5</sup> Unlike legacy private key infrastructure (PKI) technology introduced in the 1990s, *ZixCorp’s policy-based encryption* technology does not depend on the initiative of senders 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 is virtually transparent to both senders and receivers.

exclusion of enterprise mobile device usage, and the more complex threats facing enterprises, would overlook a large and quickly growing problem of data security.

Sincerely,

James F. Brashear  
Vice President, General Counsel & Secretary  
Zix Corporation  
jbrashear@zixcorp.com

cc: Glenn B. Manishin, Esq., Troutman Sanders LLP  
(glenn.manishin@troutmansanders.com)

