Federal Trade Commission
Washington, DC 20580

In the Matter of	**)**
	)
AT&T Inc.,	**)**
Verizon Wireless,	**)**
Sprint Nextel Corp., and	**)**
T-Mobile USA, Inc.	**)**

April 16, 2013

REQUEST FOR INVESTIGATION AND
COMPLAINT FOR INJUNCTIVE RELIEF

SUMMARY

1. The major wireless carriers have sold millions of Android smartphones to consumers. The vast majority of these devices rarely receive software security updates.

2. A significant number of consumers are using smartphones running a version of the Android operating system with known, exploitable security vulnerabilities for which fixes have been published by Google, but have not been distributed to consumers' smartphones by the wireless carriers and their handset manufacturer partners.

3. Android smartphones that do not receive regular, prompt security updates are defective and unreasonably dangerous. As the FTC has acknowledged, security vulnerabilities on consumers' mobile devices may be used "to record and transmit information entered into or stored on the device … to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer … [and to misuse] sensitive device functionality such as the device's audio recording feature … to capture private details of an individual's life."[1]

4. Widely distributed Android malware has exploited known security vulnerabilities in the Android operating system for which fixes from Google existed, but which the vast majority of consumer devices had not received at the time of infection.[2]

---

[1] Complaint at 6, HTC America Inc., F.T.C. No. 122 3049 (Feb. 22, 2013), available at http://ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

[2] *See An Update on Android Market Security*, Google Mobile Blog (Mar. 5, 2011), http://googlemobile.blogspot.com/2011/03/update-on-android-market-security.html ("The applications took advantage of known vulnerabilities which don't affect Android versions 2.2.2 or higher. ") *See also* http://arstechnica.com/gadgets/2011/03/google-using-remote-kill-switch-to-swat-android-malware-apps/ ("Although Google can deploy software to undo the damage caused by the malware, the underlying

5. The wireless carriers have failed to warn consumers that the smartphones sold to them are defective, that they are running vulnerable software, and that other smartphones are available that receive regular, prompt updates to which consumers could switch.

6. President Obama, the Federal Trade Commission, the National Security Agency and several other government agencies have all stressed the importance of software updates and their critical impact on the cybersecurity of consumer, business and government computer systems.[3]

7. The practices of the major wireless carriers alleged herein as they relate to the poor security of the smartphones sold to consumers constitute deceptive and unfair business practices subject to review by the FTC under section 5 of The Federal Trade Commission Act.

PARTIES

8. The American Civil Liberties Union Foundation ("ACLU") is a nationwide, non-profit, nonpartisan organization dedicated to the constitutional principles of liberty and equality. The ACLU's Project on Speech, Privacy, and Technology is dedicated to protecting and expanding the First Amendment freedoms of expression, association, and inquiry; expanding the right to privacy and increasing the control that individuals have over their personal information; and ensuring that civil liberties are enhanced rather than compromised by new advances in science and technology.

9. AT&T Inc. ("AT&T"), Verizon Wireless, ("Verizon"), Sprint Nextel Corp. ("Sprint"), and T-Mobile USA, Inc. ("T-Mobile") are the four largest wireless carriers in the United States.[4] Collectively, these four companies ("the major wireless carriers")

---

vulnerability that the attackers exploited can't be closed so easily. Google says that the bug is fixed in Android 2.2.2 and later, but there are still a large number of users at risk because their handsets runs [sic] a previous version of the operating system. Google is making a patch available, but it's going to be up to the carriers and handset makers to make sure that the patch gets deployed. In light of the mobile industry's poor track record updating Android phones, it's possible that this flaw will continue to be exploitable on a considerable number of handsets.").

[3] *See infra* notes 45-47.

[4] AT&T has 116 million wireless subscribers, while Verizon has 98 million, Sprint 55 million and T-Mobile 33 million. *See AT&T Financial and Operational Results*, AT&T (Jan. 24, 2013), *available at* http://www.att.com/Investor/Earnings/4q12/master_4q12.pdf; *Verizon Communications Financial and Operating Information*, Verizon, 13 (Dec. 31, 2012), *available at* http://www22.verizon.com/investor/DocServlet?doc=vz_4q_foi_pdf_2012_v1.pdf [hereinafter Verizon Report]; *Sprint Nextel 4Q12 Earnings Conference Call*, Sprint (Feb. 7, 2013), *available at* http://investors.sprint.com/Cache/1001172364.PDF?D=&O=PDF&iid=4057219&Y=&T=&fid=1001172364; *T-Mobile USA Reports Third Quarter 2012 Operating Results*, T-Mobile, *available at* http://www.t-mobile.com/Cms/Files/Published/0000BDF20016F5DD010312E2BDE4AE9B/5657114502E70FF3013AFB3059FB8F47/file/Q3%202012_Operating%20Results_Final.pdf.

provide service to more than 300 million subscribers, 94 percent of the US wireless market. [5]

THE FTC HAS THE AUTHORITY TO INVESTIGATE THE BUSINESS PRACTICES ALLEGED IN THIS COMPLAINT

10. Although AT&T, Verizon, Sprint and T-Mobile provide common carrier wireless telephone services, the sale of mobile computing devices such as smartphones and the provision of software updates to those devices are not common carrier activities, and are therefore subject to FTC authority under Section 5 of the FTC Act.[6]

STATEMENT OF FACTS

INTRODUCTION TO THE WIRELESS TELEPHONE INDUSTRY

11. The major wireless carriers offer service to consumers via two billing models: prepaid and postpaid. Prepaid services are offered without any contract or early termination fee for breaking the contract. In contrast, postpaid services are offered only with a contract, typically lasting two years, and are subject to an early termination fee if the subscriber wishes to terminate service early.[7]

12. In the United States, most wireless consumers subscribe to postpaid service.[8] Prepaid subscriptions account for just 20 percent of the retail subscriptions serviced by the wireless industry.[9]

---

[5] CTIA-The Wireless Association estimates that there are 321 million wireless subscriber connections in 2012. *See Background on CTIA's Semi-Annual Wireless Industry Study*, CTIA-The Wireless Association, *available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf.

[6] *See FTC Reauthorization: Hearing Before the Subcomm. on Consumer Affairs, Foreign Commerce, and Tourism of the S. Comm. on Commerce, Science and Transportation*, 107th Cong. (2002) (statement of Sheila F. Anthony, Commissioner, FTC), *available at* http://www.ftc.gov/os/2002/07/sfareauthtest.htm ("Defendants often argue that the [common carrier] exemption protects every action of a company that enjoys common carrier status. The commission firmly believes that only the common carrier activities of such companies are exempted."). *See also* Debora Platt Majoras, FTC Chairman, The Federal Trade Commission in the Online World: Promoting Competition and Protecting Consumers, Remarks Before the Progress & Freedom Foundation's Aspen Summit, 5n.5 (Aug. 21, 2006) *available at* http://www.ftc.gov/speeches/majoras/060821pffaspenfinal.pdf ("[A]n entity is treated as a common carrier under the Communications Act only with respect to services it provides on a common carrier basis…To the extent an entity provides non-common carrier services such as 'information services,' the provision of those services is subject to the FTC Act's prohibitions against engaging in deceptive or unfair practices and unfair methods of competition.").

[7] Oren Bar-Gill and Rebecca Stone, *Mobile Misperceptions*, 23 Harv. J.L. & Tech., 49, 79 (2009), *available at* http://its.law.nyu.edu/faculty/profiles/representiveFiles/Mobile%20Misperceptions_Published_C61AD240-5056-AF45-53960DAE71C1E28B.pdf.

[8] *Fifteenth Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services*, 26 FCC Recd. 9664, 9729 (June 27, 2011) [hereinafter FCC Report].

[9] *Id.* at 9767.

13. In addition to providing wireless service to consumers, the major wireless carriers also sell phones to consumers. According to estimates by industry analysts, nine out of every ten cell phones sold in the United States are sold by wireless carriers.[10] A significant percentage of the phones sold by the wireless carriers to consumers are offered at a discount, via a subsidy that will later be recouped through monthly service fees.[11]

14. As consumers have embraced smartphones, the major wireless carriers have increased their early termination fees,[12] which they have justified by citing the higher subsidy offered with these devices.[13]

15. The major wireless service providers exert significant control over the market for mobile devices.[14] The carriers are able to dictate the features included by manufacturers in phones, including the factory pre-installation of carrier specific apps,[15] as well as the removal of features that threaten the carriers' revenue stream, such as the ability to share the Internet connection of the phone with other devices ("tethering") without paying an additional fee to the wireless carrier.[16]

ANDROID AND THE SMARTPHONE MARKET

16. A majority of mobile subscribers in the United States now own a smartphone.[17] The adoption of smartphones will only increase as consumers upgrade their handsets, as

---

[10] Bar-Gill and Stone, *supra* note 7, at 70. *See also* Tim Wu, *Wireless Carterfone*, 1 Int'l J.L. & Comm., 389, 398 (2007), *available at* https://www.eff.org/sites/default/files/wu07wireless-carterfone.pdf.

[11] Bar-Gill and Stone, *supra* note 7, at 75 ("The free or heavily subsidized phone strategy pervades the U.S. cell phone market…Of course, the free phones are not really free. Carriers recoup the costs of the phones through subscription fees."). *See also* Wu, *supra* note 10, at 399; Comments of CTIA-The Wireless Association (Feb. 10, 2012), *available at* http://www.copyright.gov/1201/2012/comments/Bruce_G._Joseph.pdf ("Carriers subsidize the cost of handsets in exchange for a commitment from the customer that the phone will be used on that carrier's service (and/or that it will not be used elsewhere), so the subsidy can eventually be recouped through payment of recurring and usage charges.").

[12] Zach Epstein, *Sprint's Contract Termination Fee Balloons to $350 Ahead of iPhone 5 Launch*, BGR (Aug. 31, 2011), http://bgr.com/2011/08/31/sprints-contract-termination-fee-may-balloon-to-350-ahead-of-iphone-5-launch/; John Paczkowski, *AT&T's new early termination fee for the iPhone: $350*, CNET (May 21, 2010), http://news.cnet.com/8301-1035_3-20005684-94.html.

[13] Cecilia Kang, *Verizon jacks up early cancellation fees on smart phones*, Wash. Post (Nov. 4, 2009), *available at* http://voices.washingtonpost.com/posttech/2009/11/verizon_doubles_smart_phone_ea.html ("[Verizon's spokesperson] said the company decided to raise [early termination] fees because phones are just getting more expensive.").

[14] Bar-Gill and Stone, *supra* note 7, at 70.

[15] Priya Ganapati, *Bloatware Creeps Into Android Phones*, Wired (July 21, 2010), available at http://www.wired.com/gadgetlab/2010/07/bloatware-android-phones/.

[16] *See* Wu, *supra* note 10, at 401. *See also* Jonathan A. Zdziarski, *The Motorola v710: Verizon's New Crippled Phone*, Pen Computing, http://pencomputing.com/wireless/motorolav710.html (quoting a Verizon spokesperson stating that Bluetooth features in a Motorola phone disabled by Verizon "don't work with our business model.").

[17] *America's New Mobile Majority: A Look at Smartphone Owners in the U.S.*, Nielsen Wire (May 7, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/who-owns-smartphones-in-the-us/.

the major wireless carriers report that over 80% of the new postpaid devices they sell are smartphones.[18]

17. It is estimated that 53% of the smartphones used by wireless subscribers in the United States run Google's Android operating system.[19] In the 4th quarter of 2012, an estimated 70% of the new smartphones shipped to consumers worldwide were Android devices.[20]

18. Google creates and maintains the Android operating system. Google distributes the source code for Android via its website, where its hardware partners, developers and any other interested parties can download it.[21] As bugs and security vulnerabilities are reported to or discovered by the Android team, source code patches to Android that fix the flaws are made available to developers via Google's website.

19. Most Android devices do not run the "stock" (unmodified) version of Android created by Google. Instead, the handset manufacturers and their wireless carrier partners customize the Android operating system for each device they sell. The modifications include support for specific hardware, proprietary user interface features, software applications and services created by the manufacturer, as well as the insertion or removal of functionality at the request of the major wireless carriers.

20. The modified versions of Android created by the handset manufacturers and the wireless carriers are, in effect, unique operating systems which only these companies have the ability to update.

21. Any hardware company can create and sell a device that uses the Android operating system. However, Google has worked with select hardware partners to produce a number of flagship devices sold under the Nexus brand.

22. Although they share a single brand name, there are two different categories of Nexus devices – those sold and managed directly by Google that run the stock version of Android (hereinafter "Google-managed Nexus devices") and those sold by

---

[18] 89% of the postpaid phones sold by AT&T and 86% of those sold by Verizon in the fourth quarter of 2012 were smartphones. *See Strong Growth in Wireless and U-verse Drives Revenue and Adjusted Earnings Per Share Growth in AT&T's Fourth-Quarter Results*, AT&T (Jan. 24, 2013), http://www.att.com/gen/press-room?pid=23672&cdvn=news&newsarticleid=35937. *See also Verizon Report*, *supra* note 4, at 13.

[19] *ComScore Reports December 2012 U.S. Smartphone Subscriber Market Share*, comScore (Feb. 6, 2013), http://www.comscore.com/Insights/Press_Releases/2013/2/comScore_Reports_December_2012_U.S._Smartphone_Subscriber_Market_Share.

[20] Jon Fingas, *IDC: Android surged to 69 percent smartphone share in 2012, dipped in Q4*, Engadget (Feb. 14, 2013), http://www.engadget.com/2013/02/14/idc-android-surged-to-69-percent-smartphone-share-in-2012/; Jon Fingas, *Strategy Analytics: Android claimed 70% of world smartphone share in Q4, 2012*, Engadget (Jan. 29, 2013), http://www.engadget.com/2013/01/29/strategy-analytics-android-70-percent-share/.

[21] *See generally* Android Open Source Project, http://source.android.com/index.html.

handset manufacturers and the wireless carriers which run a customized version of Android (hereinafter "Non-Google-managed Nexus devices").

THE ANDROID UPDATE PROBLEM

23. Most Android smartphones do not receive operating system updates directly from Google, nor in many cases, do they receive regular security updates at all. As a result, most Android phones are running a version of the operating system with known, exploitable security flaws.

24. It is an accepted norm in the software industry for companies to provide regular, prompt security updates to their customers. For example, Microsoft distributes automatic security updates to Windows PCs, regardless of the manufacturer or place of purchase.[22] Likewise, Apple distributes security updates directly to Macintosh computers and iOS mobile devices such as the iPhone and iPad regardless of the place of purchase or the wireless carrier used.[23]

25. Google-managed Nexus devices receive software updates directly from Google,[24] for at least 18 months after the introduction of the device.[25] Google delivers updates to Nexus devices on a regular basis. These updates fix security vulnerabilities and bugs, as well as deliver new features.

26. Non-Google-managed Nexus devices do not – and, in fact, cannot – receive operating system updates without the participation and approval of the wireless carrier. Non-Google-managed Nexus devices and all other Android smartphones receive operating system updates only when they are made available by the device manufacturer or the wireless carrier that sold the device.

27. According to statistics published by Google, only two percent of the Android devices in use around the world are running the latest version (4.2.x) of the Android operating system.[26] In contrast, Android 2.3, which was released in 2011, is installed on approximately 44% of existing Android devices.[27]

---

[22] *See generally Windows Update*, http://windows.microsoft.com/en-us/windows/help/windows-update.
[23] *See generally Software Update*, Apple, http://www.apple.com/softwareupdate/; *iOS: How to update your iPhone, iPad, or iPod touch*, Apple, *http*://support.apple.com/kb/ht4623.
[24] *Software updates*, Google Play, http://support.google.com/googleplay/bin/answer.py?hl=en&answer=2589788 ("Devices purchased on Google Play are Pure Google and among the first to receive the latest software updates from Google…For devices purchased on Google Play, you can expect software updates to come directly from Google.").
[25] The Nexus One went on sale in January 2010. The last update was provided to consumers in October 2011. The Nexus S went on sale in December, 2010. The last update was provided to consumers in October, 2012. The CDMA version of the Galaxy Nexus went on sale through Verizon and Sprint in December 2011 and the unlocked GSM version went on sale from Google's Play Store in April, 2012. The device continues to receive security updates from Google.
[26] *Platform Versions*, Android Developers (Apr. 2, 2013), http://developer.android.com/about/dashboards/index.html.
[27] *Id*.

28. The slow rate of adoption of the most recent versions of Android does not reflect a failure by consumers to seek out and install operating system updates. Instead, it reflects the fact that for most Android smartphones in use, updates to the most recent version of the operating system simply have not been made available for consumers to install.

29. With the exception of Google-managed Nexus devices, most Android phones do not receive regular, prompt operating system updates that fix security vulnerabilities.

30. A survey by security researchers published in September 2012 reported that over half of the 20,000 Android devices they surveyed were running software with known, exploitable security vulnerabilities.[28]

31. Widely distributed Android malware has exploited known security vulnerabilities in the Android operating system for which fixes from Google existed, but which the vast majority of consumer devices had not received at the time of infection.[29]

32. The information security risks associated with the lack of timely Android updates was highlighted by the Washington Post in a recent front page story, titled "'Fragmentation' leaves Android phones vulnerable to hackers, scammers":[30]

> Fixes to known security flaws [in the Android operating system] can take many months to reach individual smartphones, if they arrive at all…. What is different about the Android line of smartphones is that there are dozens of devices made by various manufacturers, such as Samsung, LG and HTC, that tailor the software and its updates to their own specifications. Then wireless carriers, such as Verizon, AT&T and Sprint, make their own changes and test each update before sending it to consumers over their wireless networks.

33. As FTC Chief Technologist Steve Bellovin wrote in a blog post accompanying the recent HTC settlement:[31]

> With Android phones, for example, software—and hence fixes—can come from any of three parties: Google, the device manufacturer, or the wireless carrier. This, coupled with the comparatively short lifespan of many phones, has led to delays in patching and even out-of-date software being shipped

---

[28] Jon Oberheide, *Early Results from X-Ray: Over 50% of Android Devices are Vulnerable*, The Duo Bulletin (Sept. 12, 2012), https://blog.duosecurity.com/2012/09/early-results-from-x-ray-over-50-of-android-devices-are-vulnerable/.

[29] *See supra* note 2.

[30] Craig Timberg, *'Fragmentation' leaves Android phones vulnerable to hackers, scammers*, Wash. Post (Feb. 6, 2013), *available at* http://articles.washingtonpost.com/2013-02-06/business/36942653_1_android-phones-android-ecosystem-android-devices.

[31] Complaint at 6, HTC America Inc., F.T.C. No. 122 3049 (Feb. 22, 2013), *available at* http://ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

with new devices. It's easy to understand why this has happened; that said, it leaves most users without effective recourse.[32]

34. The U.S. Government Accountability Office described the same problem in a 2012 report on mobile security:

> It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.[33]

35. All of the major wireless carriers have failed to deliver regular, prompt updates to Android phones which they have sold to their customers.[34]

36. A survey in December 2012 by the technology news site Ars Technica revealed that consumers routinely have to wait for lengthy periods of time, up to 15 months after the introduction of the phone, before they receive the first Android operating system update.[35]

37. Although most of the Android devices surveyed by Ars Technica have eventually received at least one operating system update, each of the four major wireless carriers has also sold "orphaned" Android devices which did not receive any security or feature updates after they were introduced.[36]

UPDATES AND THE ANDROID BROWSER

38. In addition to running out of date operating system software with known vulnerabilities, the majority of Android phones used by consumers are also running

---

[32] Steve Bellovin, *Shipping Security*, Tech@FTC (Feb. 22, 2013), http://techatftc.wordpress.com/2013/02/22/shipping-security/.
[33] U.S. Gov't Accountability Office, GAO-12-757, Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged 19 (2012), *available at* http://www.gao.gov/assets/650/648519.pdf [hereinafter GAO Report].
[34] Casey Johnston, *The checkered, slow history of Android handset updates*, Ars Technica (Dec. 21, 2012), http://arstechnica.com/gadgets/2012/12/the-checkered-slow-history-of-android-handset-updates/.
[35] *Id.*
[36] *Id.*

an out of date, insecure version of the default Android web browser.[37] The major wireless carriers have failed to warn their customers that the default web browser included with their Android phones has known, unpatched security vulnerabilities.

39. Google's Play Store provides a mechanism through which app developers can distribute updates to consumers. Google uses the Play Store to distribute updates for Google-created Android apps, including the Google apps that are preinstalled on Android phones, such as Google Mail, Google Maps and YouTube.

40. The default browser included with the Android operating system does not use the Play Store update mechanism. Instead, the Android browser receives security updates only when the operating system is updated.

41. Although the Android default browser is rarely updated, the industry norm is for web browsers to receive regular, prompt security updates.

42. New releases of Mozilla's Firefox browser and Google's Chrome browser for PCs and Macs are automatically delivered to users every six weeks.[38] When critical security issues are discovered, both Google and Mozilla push updates to users immediately, rather than waiting for the next planned release.

43. In February 2012, Google introduced the Chrome browser app for Android, which receives regular updates through the Google Play Store.[39] Chrome for Android is pre-installed on recent Google-managed Nexus devices and on those devices, it has replaced the default Android browser. Users of other Android devices must download Chrome from the Play Store if they wish to use it.

44. Because Chrome for Android can be updated through the Play Store, Google is able to distribute regular security updates to Chrome users. However, Chrome for Android is only compatible with devices running Android 4.0 and above. As such, only 40% of the Android devices worldwide can install Chrome.

45. There exist several other free web browsers for the Android operating system, such as Firefox and Opera, which can be downloaded through the Google Play Store and regularly receive security updates.

---

[37] *See generally Top 9 Mobile Browsers in the United States from Feb 2012 to Feb 2013*, StatCountetr Global States, http://gs.statcounter.com/#mobile_browser-US-monthly-201202-201302-bar.
[38] Anthony Laforge, *Release Early, Release Often*, Chromium Blog (July 22, 2010), http://blog.chromium.org/2010/07/release-early-release-often.html. *See also Future Releases*, Mozilla, https://blog.mozilla.org/futurereleases/2011/07/19/every-six-weeks/.
[39] Sunar Pichai, *Introducing Chrome for Android*, Google Chrome Blog (Feb. 7, 2012), http://chrome.blogspot.com/2012/02/introducing-chrome-for-android.html. *See also Chrome Releases*, Google Chrome Blog, http://googlechromereleases.blogspot.com/search/label/Chrome%20for%20Android (showing frequency of new releases of Chrome for Android).

46. To date, the major wireless carriers have failed to warn their customers about known vulnerabilities in the default Android browser, nor informed them about the availability of other web browsers for Android, including Chrome, Firefox and Opera which receive regular security updates.

OUT OF DATE BROWSER SOFTWARE EXPOSES TO CONSUMERS TO CYBERSECURITY RISKS

47. The web browser is the software tool through which consumers interact with the most untrusted and potentially malicious content downloaded from the Internet. Security researchers have observed that "[i]n recent years the [w]eb browser has increasingly become targeted as an infection vector for vulnerable hosts."[40]

48. The Online Trust Alliance (OTA), an Internet industry organization, has noted that:

> Older and un-patched browsers have known vulnerabilities which cybercriminals continue to attempt to exploit… Browser vulnerabilities can lead to identity theft, installation of malicious software, or worse.[41]

49. A study in 2008 of web browser security by Swiss researchers (a team that included a Google engineer) observed that:

> [A] significant fraction of the Web browsers used to navigate the Internet on a daily basis have been identified as being not up-to-date in terms of having the latest security patches applied. As such, they put the users that rely upon them at risk and infections by malware from the Web can expose personal data stored on their hosts to attackers.[42]

50. The GAO highlighted the security risks associated with out of date mobile browsers in a recent report to Congress on mobile security threats:

> Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.[43]

---

[40] Stefan Frei, Thomas Duebendorfer, Gunter Ollmann & Martin May, *Understanding the Web Browser Threat: Examination of Vulnerable Online Web Browser Populations and the "Insecurity Iceberg"*, 288 ETH Zurich Tech Rep., *available at* http://e-collection.library.ethz.ch/eserv/eth:30892/eth-30892-01.pdf.

[41] *Why Your Browser Matters: Promoting Teachable Moments Implementation Guide*, Online Trust Alliance, 3 (Oct. 11, 2011), http://www.otalliance.org/Browser/WhyYourBroswerMatters.pdf.

[42] *Id*.

[43] GAO Report, *supra* note 33, at 20.

THE FEDERAL GOVERNMENT HAS RECOGNIZED THAT SOFTWARE UPDATES ARE A CYBERSECURITY PRIORITY

51. In published materials made available to the general public, the FTC, Federal Communications Commission, United States Computer Emergency Readiness Team (US-CERT), and the National Security Agency, all stress the importance of security updates.[44]

52. President Obama and John Brennan in his role as the President's Deputy National Security Advisor have both urged Americans to keep their software up to date.[45]

53. In a letter to the Acting Director of the Office of Management and Budget in 2012, the Federal Information Security and Privacy Advisory Board highlighted the importance of software security updates for computer systems used by Federal agencies and specifically warned about "the security risks posed by agencies' continued reliance on unsupported systems."[46]

---

[44] *Computer Security*, Onguard Online (Sept. 2011), http://www.onguardonline.gov/articles/0009-computer-security#security ("If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities.") (Onguard Online is a project of the FTC); *Cyber Security Planning Guide*, FCC, NS-2, http://transition.fcc.gov/cyber/cyberplanner.pdf ("All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems."); Jennifer Kent and Katie Steiner, *Ten Ways to Improve the Security of a New Computer*, U.S. Computer Emergency Readiness Team, 4 (2012), http://www.us-cert.gov/reading_room/TenWaystoImproveNewComputerSecurity.pdf ("Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection."); *Hardening Tips for Default Installation of Mac OS X 10.5 "Leopard"*, NSA Systems and Network Analysis Center, *available at* http://www.nsa.gov/ia/_files/factsheets/macosx_hardening_tips.pdf ("Regularly applying system updates is extremely important."). *See also Best Practices for Keeping Your Home Network Secure*, NSA Information Assurance Mission (Apr. 2011), *available at* http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf.

[45] President Barack Obama, *Protecting Yourself Online*, White House Blog at 2:10 (Oct. 15, 2009), http://www.whitehouse.gov/blog/Protecting-yourself-online/ ("There are simple steps you can take to stay safe online. Keep your security software and systems up to date."). *See also* John Brennan, *Cybersecurity Awareness Month Part III*, White House Blog (Oct. 19, 2009), http://www.whitehouse.gov/blog/Cybersecurity-Awareness-Month-Part-III ("Hackers also take advantage of Web browsers and operating system software that do not have the latest security updates. Operating system companies issue security patches for flaws that they find in their systems, so it is important to set your operating system and web browser software to download and install security patches automatically.").

[46] Letter from Daniel J. Chenok, Chair of Info. Sec. and Privacy Advisory Bd., to Jeffrey Zients, Acting Director of U.S. Office of Mgmt. and Budget (Mar. 30, 2012), *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_outdated-os.pdf.

54. The Federal Bureau of Investigation's Internet Crime Complaint Center has specifically highlighted the importance of smartphone updates in defending against device hacking and compromise.[47]

UNPATCHED, VULNERABLE SMARTPHONE SOFTWARE EXPOSES CONSUMERS, BUSINESES AND GOVERNMENT AGENCIES TO PRIVACY HARMS, CYBERCRIME AND NATIONAL SECURITY THREATS

55. In its recent settlement with smartphone manufacturer HTC, the FTC highlighted the risks faced by consumers who use mobile devices with vulnerable software.

> Because of the potential exposure of sensitive information and sensitive device functionality through the security vulnerabilities in HTC mobile devices, consumers are at risk of financial and physical injury and other harm. Among other things, malware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device, including financial account numbers and related access codes or personal identification numbers, medical information, and personal information such as text messages and photos. Sensitive information exposed on the devices could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.[48]

56. Likewise, at a Congressional hearing in 2011, then Deputy Assistant Attorney General Jason Weinstein stressed the Department of Justice's concern about mobile phones and cybercrime, telling the committee that mobile devices "are increasingly tempting targets for identity thieves and other criminals" and that "Americans who are using infected computers and mobile devices are suffering from an extensive, pervasive invasion of their privacy at the hands of these criminals almost every single time they turn on their computers."[49]

---

[47] *Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and Safety Measure to Help Avoid Compromise*, Internet Crime Complaint Center Intelligence Note (Oct. 12, 2012), http://www.ic3.gov/media/2012/121012.aspx.

[48] Complaint at 6, HTC America Inc., F.T.C. No. 122 3049 (Feb. 22, 2013), *available at* http://ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

[49] *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on Judiciary*, 112th Cong. (2011) (testimony of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), video at approx. 41:00, http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary051011&st=xxx ("As the use of mobile devices continues to grow, these devices are increasingly tempting targets for identity thieves and other criminals…From around the corner or around the globe, skilled computer hackers work every single day to access computer systems and mobile devices of government agencies, universities, banks, merchants, credit card companies to steal large volumes of personal information, to steal intellectual property, and to perpetrate large scale data breaches that leave tens of millions of Americans at risk of

57. In 2012, the House Intelligence Committee held a hearing focused on national security threats posed by the domestic use of Chinese telecommunications equipment, including smartphones, made by Huawei and ZTE, two of the largest device manufacturers in the world. In his opening remarks, Committee Chairman Mike Rogers made it clear that "Americans have to trust our telecommunications networks" and that "[w]hen vulnerabilities in the equipment, such as backdoors and malicious code can be exploited by another country, it becomes a priority and a national security concern."[50]

58. When questioned by Committee Chairman Rogers about media reports of covert backdoors that had been discovered in the Android operating system installed on ZTE's smartphones,[51] ZTE's Senior Vice President for North America and Europe Zhu Jinyun told the committee that:

> What [the US media] have been calling backdoors are actually software bugs and these are the sorts of bugs you'll find in all high tech companies. For instance, companies like Microsoft, like Google, like Apple have all had these bugs in their software. And that is why we always, like they, periodically and non-periodically, issue patches to these software bugs as soon as they're discovered. [52]

59. In response, Chairman Rogers' observed that "one person's bug is yet another's backdoor." In other words, whether intentionally placed or not, unpatched software flaws in telephone handsets are, in fact, a serious national security threat.

THE STANDARD FOR DETERMINING THAT A BUSINESS PRACTICE IS DECEPTIVE

60. Section 5 of the FTC Act prohibits deceptive acts and practices in advertising.[53] There are three elements to a deception case. First, there must be a representation, omission, or practice that is likely to mislead the consumer. Second, the act or practice must be evaluated from the perspective of a reasonable consumer. Third, the representation, omission, or practice must be material.[54]

---

identity theft…[Mobile] devices provide yet another computing platform for cybercriminals to target for botnets and infection by malicious code. Unfortunately, American who are using infected computers and mobile devices are suffering from an extensive, pervasive invasion of their privacy at the hands of these criminals almost every single time they turn on their computers.").

[50] RepMikeRogers, *Huawei and ZTE Testify Before the House Intel Committee Part 1*, YouTube at 4:17 (Oct. 3, 2012), http://www.youtube.com/watch?v=ApQjSCUpt4s.

[51] Jeremy Wagstaff and Lee Chyen Yee, *ZTE confirms security hole in U.S. phone*, Reuters (May 18, 2012), http://www.reuters.com/article/2012/05/18/us-zte-phone-idUSBRE84H08J20120518.

[52] RepMikeRogers, *Huawei and ZTE Testify Before the House Intel Committee Part 2*, YouTube at 28:23 (Oct. 3, 2012), http://www.youtube.com/watch?v=wG2tk98AX_s.

[53] 15 U.S.C. § 45 (West).

[54] *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 170–71 (1984).

61. With respect to the first element, as the Commission noted in the landmark *Cliffdale Associates* case, "[p]ractices that have been found misleading or deceptive in specific cases include false oral or written representations, misleading price claims, *sales of hazardous or systematically defective products or services without adequate disclosures*, failure to disclose information regarding pyramid sales, use of bait and switch techniques, failure to perform promised services, and failure to meet warranty obligations."[55]

62. With respect to the third element, "a material representation, omission, act or practice involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product. Consumers thus are likely to suffer injury from a material misrepresentation."[56]

THE MAJOR WIRELESS CARRIERS' FAILURE TO PROVIDE UPDATES TO CONSUMERS USING NON-GOOGLE-MANAGED ANDROID PHONES IS A DECEPTIVE AND UNFAIR BUSINESS PRACTICE

63. As noted above, all four of the major wireless carriers consistently fail to provide consumers with available security updates to repair known security vulnerabilities in the software operating on mobile devices.

64. The wireless carriers have failed to warn consumers that the smartphones sold to them are defective and that they are running vulnerable operating system and browser software.

65. The delivery of software updates to consumers is not just an industry best practice,[57] but is in fact a basic requirement for companies selling computing devices that they know will be used to store sensitive information, such as intimate photographs, email, instant messages, and online banking credentials.

66. As FTC Chief Technologist Steve Bellovin wrote in a blog post accompanying the recent HTC settlement:

> "[Not delivering updates] is a non-starter for most security holes, since those can become critical, recurring problems any time some attacker wants them to."

---

[55] *Id.* (emphasis added).

[56] *Id.*

[57] Frei et al., *supra* note 40, at 3 ("For years the software industry has promoted one security best practice over all others: always use the most recent version of the installed software and instantly apply the latest patches. With today's hostile Internet and drive-by download attack vectors, failure to apply patches promptly or missing them entirely is a recipe for disaster; exposing the host to infection and possibly subsequent data disclosure or loss.")

Summarizing the situation, Bellovin wrote that "[b]ugs happen, ergo fixes have to happen."

67. A substantial percentage of consumers who purchased carrier-supplied non-Google-managed Android smartphones within the last two years are postpaid subscribers still under contract.[58] Many of these consumers are using smartphones with known, exploitable software vulnerabilities for which the major wireless carriers have not supplied a security update.

68. Wireless carriers continue to extract monthly fees, part of which is repayment for the carrier's initial phone subsidy,[59] for smartphones that the carriers know to be defective.

69. In spite of the fact that their devices are vulnerable, these consumers remain locked into their wireless service contracts, which are enforced by prorated early termination fees.[60]

70. Wireless carriers' sale of Android smartphones to consumers and subsequent failure to provide consumers with available security updates constitutes the sale of systematically hazardous products, without adequate disclosures that consumers will be subject to such critical vulnerabilities. This omission constitutes a misleading and deceptive practice under Section 5 of the FTC Act.

71. Consumers reasonably expect that the operating system software on their phones will receive prompt, regular security updates.

72. By failing to provide consumers with critical security updates for smartphones which they pay off each month, the wireless carriers have exposed consumers to risk of substantial harm.

73. The only reasonable way for most consumers to avoid this harm would be to either a) break their contract, pay the remaining prorated portion of the early termination fee and buy a new smartphone, or b) buy a new unsubsidized device to use under their existing contract, while continuing to make monthly payments and pay off the subsidy for the vulnerable phone that they will no longer use.

---

[58] *See supra* ¶¶ 16-18.

[59] Wu, *supra* note 10, at 399. *See also* Comments of CTIA-The Wireless Association (Feb. 10, 2012), *available at* http://www.copyright.gov/1201/2012/comments/Bruce_G._Joseph.pdf ("Carriers subsidize the cost of handsets in exchange for a commitment from the customer that the phone will be used on that carrier's service (and/or that it will not be used elsewhere), so the subsidy can eventually be recouped through payment of recurring and usage charges.").

[60] Early termination fees act as a form of lock-in, effectively preventing many consumers from switching to a competing wireless carrier. *See* Bar Gill *supra* note 7, at 55 ("Lock-in prevents efficient switching and thus hurts consumers. One survey found that 47% of subscribers would like to switch plans, but only 3% do so — the rest are deterred by the ETF.").

74. Wireless carriers' exposure of their customers to the risk of substantial harm renders the omission with respect to security vulnerabilities a material omission.

75. Moreover, the enforcement of wireless service contract early termination fees for subscribers with vulnerable smartphones is an unfair business practice, because it unreasonably penalizes consumers whose private information can no longer be safely stored on the vulnerable smartphones sold to them by their wireless carrier.

REQUEST FOR RELIEF

The ACLU requests that the Commission investigate the major wireless carriers and enjoin their unfair and deceptive business practices. Specifically, the ACLU requests that the Commission:

A. Compel the major wireless carriers to warn all subscribers using carrier-supplied Android smartphones with known, unpatched security vulnerabilities about the existence and severity the vulnerabilities, as well as any reasonable steps those consumers can take to protect themselves, including purchasing a different smartphone.

B. Compel the major wireless carriers to permit consumers under contract who are using carrier-supplied Android smartphones which have not received prompt, regular security updates to end their contracts early, without any early termination fee.

C. Compel the wireless carriers to permit consumers who are using carrier-supplied Android smartphones less than two years old which have not received prompt, regular security updates to either:

    1. Exchange, at no cost, their existing device for another phone that will receive prompt, regular updates directly from Apple, Google, Microsoft or another mobile operating system vendor.

    2. Return the phone and receive a full refund of the original purchase price.

Respectfully submitted,

Christopher Soghoian
Principal Technologist and Senior Policy Analyst
Speech, Privacy & Technology Project
American Civil Liberties Union Foundation
915 15th St NW
Washington, DC 20005
csoghoian@aclu.org

Ben Wizner
Director
Speech, Privacy & Technology Project
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor,
New York NY 10004