Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)
	)
"Verizon Wireless"	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center

I. Introduction

1. This complaint concerns material changes to the business practices of "Verizon Wireless," the second-largest mobile phone carrier in the United States, that have adversely impacted the privacy interests of the company's customers. After consumers entered into long-term contracts with Verizon Wireless, the company changed its data use and disclosure practices, making the personal information of its customers more widely available to others. Moreover, Verizon represents that the information that it discloses to others cannot be linked to its customers but provides no basis whatsoever for this assurance. Such practices are unfair and deceptive, contrary to the privacy and security interests of Verizon Wireless customers, and actionable by the Federal Trade Commission.

2. Eighty-eight percent of Verizon's users enter into long-term contracts with Verizon Wireless, most of which run for two years. Every contract includes a penalty for early cancellation, which can be as high as $350.

3. Verizon Wireless represented to these consumers that the company would not collect or distribute users' location data, web browsing histories, internet search terms, demographic information, and mobile device usage information. The company stated that it would provide "clear and meaningful notice of our practice and obtain [consumers'] affirmative consent" before changing its information and disclosure practices.

4. Without obtaining the affirmative consent of its users, Verizon Wireless subsequently altered its business practices, collecting and distributing users' location data, web browsing histories, internet search terms, demographic information, and mobile device usage information.

5. Furthermore, Verizon Wireless described the company's changes so as to falsely assure consumers that it was not disclosing "any information that identifies [the user] personally." Users' location data, web browsing histories, internet search terms, demographic information, and mobile device usage information are often personally identifiable.

6. Verizon Wireless's collection and disclosure of this personal information violates user expectations, diminishes user privacy, and contradicts Verizon Wireless's own representations.

7. These business practices are Unfair and Deceptive Trade Practices, subject to review by the Federal Trade Commission (the "Commission") under section 5 of the Federal Trade Commission Act.

8. These business practices impact approximately 100 million Verizon Wireless customers, consumers who fall within the jurisdiction of the United States Federal Trade Commission.[1]

9. EPIC urges the Commission to investigate Verizon Wireless, determine the extent of the harm to consumer privacy and safety, require Verizon Wireless to immediately cease its unfair and deceptive data collection and disclosure practices, delete all data collected pursuant to the recent changes, ensure that all data disclosed by Verizon Wireless pursuant to the recent changes is deleted by the recipients; implement an opt-in consent model for all future changes to the company's data collection and disclosure practices, and provide such other relief as the Commission finds necessary and appropriate.

II. Parties

10. The Electronic Privacy Information Center ("EPIC") is a not-for-profit research center based in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the Federal Trade Commission. EPIC first brought the Commission's attention to privacy risks of targeted marketing and then to the privacy risks of online advertising.[2] In 2004, EPIC filed a complaint with the FTC regarding the deceptive practices of data broker firm Choicepoint, which had failed to safeguard consumer information in the firm's possession.[3] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million, the largest fine in the history of the FTC at the time.[4] EPIC also initiated the complaint to the FTC regarding Microsoft Passport.[5] The Commission subsequently required Microsoft to implement a

[1] *About Us*, http://aboutus.verizonwireless.com/ataglance.html (last visited Oct. 26, 2011).
[2] DoubleClick, Inc., __ F.T.C __ (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.
[3] Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.
[4] Federal Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm.
[5] Microsoft Corporation, (July 26, 2001) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), *available at* http://epic.org/privacy/consumer/MS_complaint.pdf.

comprehensive information security program for Passport and similar services that reduced the risk of the profiling of Internet users.[6] EPIC filed a complaint with the FTC regarding the marketing of amateur spyware,[7] which resulted in the issuance of a permanent injunction barring sales of CyberSpy's "stalker spyware," over-the-counter surveillance technology sold for individuals to spy on other individuals.[8] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning the social networking service.[9] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[10]

11. Cellco Partnership is a Delaware partnership doing business as "Verizon Wireless."[11] Verizon Wireless is a voice and data services company headquartered in Basking Ridge, NJ.[12] The company was formed in 2000 as the result of a joint venture between Verizon, Inc. and Vodafone Group, Plc. ("Vodafone").[13] Verizon, Inc. owns a 55 percent interest in Verizon Wireless, and Vodafone owns the remaining 45 percent.[14]

III. Factual Background

A. Verizon Wireless' Business Practices Impact More than 100 Million Consumers

12. In 2010, Verizon Wireless claimed annual revenue of $63.4 billion, representing 60 percent of Verizon, Inc.'s aggregate revenue.[15]

---

[6] Microsoft Corporation, File No. 012 3240, Docket No. C-4069 (2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm; *see also* Fed. Trade Comm'n, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), http://www.ftc.gov/opa/2002/08/microsoft.shtm.

[7] Awarenesstech.com, et al., __ F.T.C. __ (2008) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), *available at* http://epic.org/privacy/dv/spy_software.pdf.

[8] *FTC v. Cyberspy Software*, No. 6:08-cv-1872 (D. Fla. Nov. 6, 2008) (unpublished order), http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.

[9] Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").

[10] *Id.*

[11] Cellco Partnership, 10-K filing to the US Securities and Exchange Commission, Mar. 12, 2010, available at http://news.verizonwireless.com/investor/pdf/Cellco-Partnership-2009-Form-10-K.pdf

[12] *About Us*, http://aboutus.verizonwireless.com/ataglance.htmlhttp://aboutus.verizonwireless.com/ataglance.html (last visited Oct. 26, 2011).

[13] Verizon Communications, Inc., Annual Report 3 (Form 10-K) (Feb. 28, 2011), http://eol.edgarexplorer.com/EFX_dll/EDGARpro.dll?FetchFilingHTML1?SessionID=XukkiWhUFX_cXzg&ID=7759054.

[14] *Id.*

[15] Id.

13. Verizon Wireless has over 100 million customers, 89.7 million of whom are retail customers.[16] Consumers access Verizon Wireless's network using a variety of devices, including smartphones, tablets, and computers.

14. Consumers of Verizon Wireless's devices or services enter into term, month-to-month, or prepaid contracts with the company.[17]

15. Eighty-eight percent of Verizon Wireless's customers are locked into term contracts with the company. The majority of these contracts run for two years. [18]

16. Verizon Wireless' term contracts contain early termination penalties, which the company calls "Early Termination Fees" ("ETF").[19] Verizon Wireless' ETFs can be as high as $350.[20] Thus, consumers are effectively locked into their long-term contracts.

B. After Locking Consumers into Long-Term Contracts, Verizon Wireless Unilaterally Altered the Company's Personal Data Collection and Disclosure Policies, Collecting and Revealing Consumers' Personal Information that was Previously Kept Confidential

17. Prior to October 14, 2011, Verizon Wireless assured consumers that it would not collect or disclose personal information concerning customers' location data, web addresses and search terms, demographic information, and mobile device usage.

18. In selecting the Verizon service over the service of other competing carriers, consumers relied upon the representations made by Verizon regarding the protection of personal information that the company would obtain from the consumer.

19. In the absence of a statutory obligation to regulate Verizon's data collection practices, the representations that the company made regarding its data collection practices was in fact the only privacy safeguard for consumers.

20. The company's Customer Agreement stated that "[Verizon Wireless] *may* collect personal information about you,"[21] but did not notify consumers that the company collected customers' location data, web addresses and search terms, demographic

---

[16] *About Us*, http://aboutus.verizonwireless.com/ataglance.html (last visited Oct. 26, 2011).http://aboutus.verizonwireless.com/ataglance.html

[17] Most cell phone consumers use term contracts, although the adoption rate of prepaid service plans has increased in recent years. *See* New Millennium Research Center, Recession has Cell Phone Consumers' Number, as Two out of Three New Wireless Subscribers in US Go Prepaid (Mar. 31, 2010), http://newmillenniumresearch.org/news/033110_prepaid_trends_news_release.pdfhttp://newmillenniumresearch.org/news/033110_prepaid_trends_news_release.pdf.

[18] Verizon Communications, Inc., *supra* note 12, at 3.

[19] *See* Letter from Kathleen Grillo, Verizon Wireless, to Joel Gurin and Ruth Milkman, Federal Communications Commission (Feb. 23, 2010) http://transition.fcc.gov/cgb/etf/VerizonWirelessETFResponse.pdf.

[20] *http://transition.fcc.gov/cgb/etf/VerizonWirelessETFResponse.pdfId.*

[21] Verizon Wireless, *Customer Agreement*, VERIZON WIRELESS (Feb. 25, 2011), http://web.archive.org/web/20110225151331/https://www.verizonwireless.com/b2c/globalText?textName=CUSTOMER_AGREEMENT&jspName=footer/customerAgreement.jsp (emphasis added).

information, and mobile device usage. As such, the Verizon notice failed to provide the consumer any useful information on which the consumer could meaningfully assess the company's practices.

21. Verizon Wireless' Customer Agreement directed consumers to the company's "Privacy Policy" for more information about the types of information that the company collected.[22]

22. The company's Privacy Policy did not mention the disclosure of web addresses and location data to third parties for business and marketing purposes.[23]

23. In fact, Verizon Wireless's Privacy Policy assured consumers that the company did not collect data concerning consumers' web usage, stating, "Verizon does not gather information from your use of our broadband access services to determine your Web surfing activities across non-Verizon sites for the purpose of providing you with interest-based advertisements. *If Verizon engages in this type of online behavioral advertising, we will provide you with clear and meaningful notice of our practice and obtain your affirmative consent.*"[24] (emphasis added)

24. On October 14, 2011, Verizon Wireless announced that the company had changed its practices concerning collection and disclosure of users' personal information.[25]

25. The company stated that it had started collecting its customers' location data, web addresses and search terms, demographic information, and mobile device usage. The company further stated that it had started disclosing this personal information to third-parties, ostensibly for marketing purposes.[26]

26. On October 17, 2011, Verizon Wireless sent an email to its customers concerning the company's expanded collection and distribution of users' personal information.[27]

27. Verizon Wireless' actions in the wake of the October 14, 2011 announcement confirm that the company made material alterations to the manner in which it collected and disclosed users' personal information.

28. After Verizon Wireless altered its business practices, the company modified its Customer Agreement to read: "We collect personal information about you."[28]

---

[22] Verizon Wireless, *Customer Agreement*, VERIZON WIRELESS (Oct. 26, 2011), https://www.verizonwireless.com/b2c/globalText?textName=CUSTOMER_AGREEMENT&jspName=footer/customerAgreement.jsp. ("You can find out how we use, share and protect the information we collect about you in the Verizon Privacy Policy, available at verizon.com/privacy.").

[23] *See* Verizon Wireless, *Privacy Policy*, VERIZON WIRELESS (Jul. 10, 2010), http://web.archive.org/web/20100710202206/http://www22.verizon.com/about/privacy/policy/#outsideVz.

[24] *Id.*

[25] Julia Greenberg, *Verizon Begins Tracking Cellphone Activity: Web Use, Location, and Apps*, International Business Times, Oct. 14, 2011, available at http://www.ibtimes.com/articles/230862/20111013/verizon-wireless-private-policy-cellphone-mobile-users-web-browsing-location-apps-google-facebook-ao.htm.

[26] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information.

[27] *Id*.

[28] Verizon Wireless, *supra* note 21.

29. After Verizon Wireless altered its business practices, the company modified its Privacy Policy to read: "As described in more detail in other sections of this policy, Verizon also may share certain information with outside companies to assist with the delivery of advertising campaigns, or preparing and sharing aggregate business and marketing reports."[29]

30. The company now collects users' personal information to "to prepare business and marketing reports that we may use ourselves or share with others."[30]

31. The company now combines users' personal information with other data obtained by the company to "determine whether you fit within audience an advertiser is trying to reach."[31]

32. The company now allows third parties to conduct "advertising that is customized based on predictions generated from your visits over time and across different websites."[32]

33. Verizon Wireless's new data collection and disclosure policy states that the company discloses two new categories of personal information: mobile usage information and consumer information.[33]

34. Mobile usage information includes: (1) the URLs of websites that a user visits, including search terms entered; (2) geolocation information; and (3) "[a]pp and device feature usage."[34]

35. Consumer information includes: (1) the type of device, amount of usage, and type data plan that a consumer uses; and (2) demographic information, such as age, gender, and interests.[35]

36. The new policy also details the ways in which this newly-collected personal information is used by Verizon Wireless and third-party companies, including (1) creating business and marketing reports that are used by Verizon Wireless or disclosed to others; (2) allowing other businesses to use geolocation information to create business and marketing reports; and (3) allowing advertisers to use demographic information to target ads.[36]

---

[29] Verizon Wireless, *Privacy Policy*, VERIZON WIRELESS (Oct. 26, 2011), https://www22.verizon.com/about/privacy/policy/#outsideVz.
[30] Appendix A.
[31] Id.
[32] *Id.*
[33] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information
[34] *Id.*
[35] *Id.*
[36] *Id.*

37. Verizon Wireless claims that none of the information collected and disclosed can identify the user personally, however the company has failed to make public the technique it has adopted to ensure this safeguard.[37]

38. Verizon Wireless did not seek customers' consent to the new collection and disclosure practices. Instead, the company collected and disclosed all users' personal information, while requiring users to opt-out of the regime if they objected to the new practices.

39. The online opt-out process requires users to check radio buttons indicating (1) their opt-out preference for each phone line on the account; and (2) which specific disclosures they wish opt out of (marketing reports or mobile advertising).[38]

C. Verizon Wireless's Information Disclosure Notice is False and Misleading Because the Company Discloses Information that is Personally Identifiable

40. The Commission recognizes that personally identifiable information ("PII") is information that is linked or could be reasonably linked to an individual.[39]

41. Verizon Wireless's information disclosure notice states that it collects and discloses information about "the location of [a user's] device" and "addresses of websites [users] visit" including "URLs" and "search terms [the user] has used."[40]

42. The Commission considers geolocation information to be personally identifiable information. In response to technological changes, the increased use of mobile devices, and new business practices, the Commission proposed amendments to the Children's Online Privacy Protection Act ("COPPA") Rule to make clear that "personal information" includes geolocation information.[41]

43. Recent studies demonstrate that web addresses can be used to personally identify users.[42]

44. AOL and Netflix have released improperly anonymized data sets consisting of users' web search terms and video ratings. Bloggers and the media have been able to personally identify individual consumers using these data sets.[43]

45. The Commission has previously held companies accountable for their representations regarding the de-identification of customer data. In Liberty Financial, the Commission found that a company made false and misleading representations about the privacy of the consumer information that it collected. The company made representations that "[a]ll of [the user's] answers will be totally anonymous." In fact, the company "d[id] not maintain

[37] *Id.*
[38] *See infra* Appendix B: Customer Privacy Settings.
[39] *See infra* Part III.C.1.
[40] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information.
[41] *See infra* Part III.C.2.
[42] *See infra* Part III.C.3.
[43] *Id.*

the information it collects . . . in an anonymous manner because individuals can be identified with their responses to the survey."[44]

1. Personally Identifiable Information is Information That is Linked or Could be Reasonably Linked to an Individual

46. The Commission has recognized that PII is information that is linked or could reasonably be linked to an individual.

47. The Commission's 2010 report on a proposed privacy framework for businesses and consumers states that the proposed framework "applies to those commercial entities that collect data that can be reasonably linked to a specific consumer, computer, or other device."[45]

48. The Commission's report on behavioral advertising concludes that companies should extend behavioral advertising protections to any data that can be reasonably linked to a specific consumer, computer, or other device.[46]

49. The Commission's Health Breach Notification Rule requires entities to provide breach notification to an individual if they have a reasonable basis to believe the data can be linked to that individual.[47]

50. The European Union's Article 29 Data Protection Working Party and the OECD Privacy Guidelines also define PII in a way that includes information that can reasonably be linked to an individual.[48]

51. It is necessary to place the burden on the service provider to demonstrate that it is not possible to reconstruct user identity.[49]

---

[44] *See infra* Part III.C.4.

[45] FEDERAL TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 43 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[46] FEDERAL TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 42 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[47] 16 C.F.R. § 318 (2009).

[48] *See* Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 6, 01248/07/EN/WP 136 (June 20, 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. (PII includes four elements: (1) any information (2) relating to (3) an identified or identifiable (4) natural person. The Working Party's Opinion states that information is PII when, "although the person has not been identified yet, it is possible to do it."); see also OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html#part1 (defining personal data as simply "any information relating to an identified or identifiable individual.").

[48] *Id.* at 12.

[49] Testimony and Statement for the Record of EPIC Executive Director Marc Rotenberg on ""Communications Networks and Consumer Privacy: Recent Developments" before the House Committee on Energy and Commerce, Apr. 23, 2009 ("Without this statutory obligation, there would be no practical consequence if a company inadvertently disclosed personal information or simply changed its business model to true user-based profiling.")

2. Geolocation Data is Personally Identifiable Information

52. Verizon Wireless' new policy states that it collects and discloses information about "the location of [a user's] device."[50] Verizon Wireless claims that this information does not identify users personally but does not reveal the techniques that ensure this protection.

53. The Commission recognizes that geolocation information is linked or could reasonably be linked to an individual.

54. The Commission's amendments to the Children's Online Privacy Protection Act ("COPPA") Rule updates the definition of Personally Identifiable Information in response to changes in technology, the increased use of mobile devices, and new business practices.[51] Under the new Rule, "personal information" includes "geolocation information."[52]

55. The Commission's COPPA Rule recognizes that geolocation information allows a company to be able to contact a specific individual, even without collecting other identifying information.[53] In fact, geolocation information "may be more precise than street name and name of city or town."[54]

56. The European Commission's Article 29 Working Party recently issued an Opinion on geolocation data and mobile devices concluding that geolocation information was personally identifiable information. [55]

57. Restrictions on the collection of location information are appropriate to protect privacy and ensure personal mobility.[56]

3. Web Addresses and Search Term Data are Personally Identifiable Information

58. Verizon Wireless also collects and discloses "addresses of websites [users] visit" including "URLs" and "search terms [the user] has used."[57] As with geolocation information, the company claims that this data does not identify users personally. However, recent studies and the experiences of companies such as AOL and Netflix reveal that web addresses and search term data are linked or could reasonably be linked to an individual consumer.

---

[50] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information.
[51] Federal Trade Comm'n, FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule (Sept. 15, 2011), http://www.ftc.gov/opa/2011/09/coppa.shtm.
[52] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59813 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312), http://www.ftc.gov/os/2011/09/110915coppa.pdf.
[53] *Id.* at 59811.
[54] *Id.* at 59813.
[55] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices 13, 881/11/EN/WP 185 (May 16, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[56] Marc Rotenberg, "Communications Privacy: Implications for Network Design," 36 *Communications of the ACM* 61, 68 (August 1993).
[57] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information.

59. Personally identifiable information may be revealed through web address data, including "[p]otentially identifying demographic information (gender, ZIP, interests) in the Request-URI" and "[u]sername or real name in page title."[58]

60. An example from Sports.com "contain[ed] the user's *email address in the URL*."[59]

61. Furthermore, a company in possession of the browsing history of users could "deanonymize" it by correlating the data to external information.[60]

62. Personally identifiable information is frequently revealed "when a first-party website stuffs information into a URL."[61] For example, Photobucket embeds usernames in URLs; other URLs may contain a usernames, "real" names, or email addresses.[62]

63. Usernames, which are most frequently disclosed in URLs, can be used to personally identify users.[63]

64. Companies that have released improperly anonymized data have quickly discovered the ease with which it can be used to identify an individual.

65. Researchers and bloggers were able to personally identify individuals using a dataset released by AOL that contained web search queries, despite the fact that AOL had replaced subscriber names or user IDs with pseudonymous identification numbers.[64]

66. Similarly, researchers were able to reconstruct user identity after Netflix published "blinded" information about 500,000 customers. As with AOL, researchers using other

---

[58] Arvind Narayanan, *There is no Such Thing as Anonymous Online Tracking*, STANFORD CENTER FOR INTERNET & SOC'Y (July 28, 2011 12:38pm), http://cyberlaw.stanford.edu/node/6701.
[59] *Id.* (emphasis original)
[60] *Id.*
[61] Jonathan Mayer, *Tracking the Trackers: Where Everybody Knows Your Username*, STANFORD CENTER FOR INTERNET & SOC'Y (Oct. 11, 2011 8:06am), http://cyberlaw.stanford.edu/node/6740.
[62] *Id.*
[63] Id. Mayer explained in detail the ways in which usernames constitute identifying information. First, in many cases, consumers simply use their names to create usernames. Second, even when consumers create wholly fictitious usernames, they often routinely reuse them on different sites, and thus the usernames may become linked across websites. In fact, "simple algorithms for linking usernames could achieve pairwise precision and recall of over 70%" and companies such as Infochimps, Spokeo, and Google are already linking usernames in their products. Id. Additionally, "combining data from multiple accounts often provides a sufficiently comprehensive mosaic to identify an individual." Id. A search for Narayanan's username, for example, "turned up his yCombinator Hacker News account, which includes his job and links to his personal website, blog, and Twitter account." Id. Finally, Mayer pointed out that some websites, such as Quantcast, already include username in their definition of personally identifiable information. Id.
[64] *See, e.g.*, Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&scp=1&sq=aol%20queries&st=cse&oref=slogin; Ellen Nakashima, *AOL Takes Down Site With Users' Search Data*, WASH. POST. (Aug. 8, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080701150.htm.

publicly available information were able to personally identify specific Netflix customers and thus discover information about the films they had rented.[65]

67. Other studies have also demonstrated the ease with which improperly anonymized data is in fact personally identifiable.[66]

4. The Commission has Previously Held Companies Accountable for Their Misrepresentations Regarding the De-Identification of Customer Data

68. In Liberty Financial Companies, Inc., the Commission found that a company made false and misleading representations about the privacy of the consumer information that it collected. The company created an online survey that collected personal and financial information from minors while promising that "[a]ll of [the user's] answers will be totally anonymous."[67] In fact, the company "d[id] not maintain the information it collect[ed] at the Measure Up Survey area in an anonymous manner because individuals c[ould] be identified with their responses to the survey."[68] The company also stated that users who took the survey would be entered into a contest and would receive an e-mail newsletter, neither of which actually existed.[69]

69. The Commission also held Microsoft accountable for violations associated with the Microsoft Passport identification and authentication system that collected users' personal information in connection with making purchases.[70] The case arose from the company's false representations about how personal information was protected, the security of making purchases through the Passport system, the limitations on collecting personal information other that described in the policy, and the extent of parental control over what information participating websites could collect about their children.[71]

70. In 2004, the FTC charged Gateway Learning Corporation with making a material change to its privacy policy, allowing the company to share users' information with third parties, without first obtaining users' consent.[72] This was the first enforcement action to

---

[65] *See* Bruce Schneier, *Why "Anonymous" Data Sometimes Isn't*, WIRED (Dec. 13, 2007), http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213; *see also* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf.

[66] *See* Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets, The Univ. of Texas at Austin, http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); *see also* Latanya Sweeney, Comments to the Department of Health and Human Services on "Standards of Privacy of Individually Identifiable Health Information" (Apr. 26, 2002), *available at* http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.pdf.

[67] Liberty Financial Companies, Inc., FTC File No. 982 3522, Docket No. C-3891 (1999) (complaint), *available at* http://www.ftc.gov/os/1999/08/libertycmp.pdf.

[68] *Id.*

[69] *Id.*

[70] Microsoft Corporation, File No. 012 3240, Docket No. C-4069 (2002) (decision and order), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftdecision.pdf.

[71] Microsoft Corporation, File No. 012 3240, Docket No. C-4069 (2002) (complaint), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf.

[72] Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004),

"challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[73] Gateway Learning made representations on the site's privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.[74] In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.[75] Gateway then revised its privacy policy to provide for the renting of consumer information "from time to time," applying the policy retroactively.[76]

IV. Legal Analysis

A. The FTC's Section 5 Authority

71. The FTC Act prohibits unfair and deceptive acts and practices, and empowers the Commission to enforce the Act's prohibitions.[77] These powers are described in FTC Policy Statements on Deception[78] and Unfairness.[79]

72. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[80]

73. The injury must be "substantial."[81] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[82] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[83] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[84] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[85] Finally, "the injury must be one which consumers could not

---

http://www.ftc.gov/opa/2004/07/gateway.shtm.
[73] *Id.*
[74] Gateway Learning Corp., Docket No. C-4120 (2004) (complaint), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.
[75] *Id.*
[76] *Id.*
[77] *See* 15 U.S.C. § 45 (2010).
[78] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC Deception Policy].
[79] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC Unfairness Policy].
[80] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[81] FTC Unfairness Policy, *supra.*
[82] *Id.*; *see, e.g.*, *Fed. Trade Comm'n v. Information Search, Inc.*, Civ. No. 1:06-cv-01099 (Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers.").
[83] FTC Unfairness Policy, *supra.*
[84] *Id*.
[85] *Id*.

reasonably have avoided."[86] This factor is an effort to ensure that consumer decision making still governs the market by limiting the FTC to act in situations where seller behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[87] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[88]

74. The FTC will also look at "whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise."[89] Public policy is used to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[90]

75. An act or practice is deceptive if it involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment."[91]

76. There are three elements to a deception claim. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[92] The relevant inquiry for this factor is not whether the act or practice actually misled the consumer, but rather whether it is likely to mislead.[93]

77. Second, the act or practice must be considered from the perspective of a reasonable consumer.[94] "The test is whether the consumer's interpretation or reaction is reasonable."[95] The FTC will look at the totality of the act or practice and ask questions such as "how clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[96]

78. Finally, the representation, omission, or practice must be material.[97] Essentially, the information must be important to consumers. The relevant question is whether consumers would have chosen another product if the deception had not occurred.[98] Express claims

---

[86] *Id*.
[87] *Id*.
[88] *Id*.
[89] *Id*.
[90] *Id*.
[91] FTC Deception Policy, *supra*.
[92] FTC Deception Policy, *supra* ; *see, e.g.*, *Fed Trade Comm'n v. Pantron I Corp.*, 33 F.3d 1088 (9th Cir. 1994) (holding that Pantron's representation to consumers that a product was effective at reducing hair loss was materially misleading, because according to studies, the success of the product could only be attributed to a placebo effect, rather than on scientific grounds).
[93] FTC Deception Policy, *supra*.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*

will be presumed material.[99] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[100]

79. The FTC presumes that an omission is material where "the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false . . . because the manufacturer intended the information or omission to have an effect."[101]

B. Verizon Wireless' Collection and Disclosure of Users' Personal Data Constitutes an Unfair and Deceptive Trade Practice

80. As set forth above, Verizon Wireless induced consumers to enter into two-year contracts while representing that the company would not collect or distribute users' personal web browsing or search histories.

81. Verizon Wireless drafted such contracts to include substantial penalties if users elect to terminate the agreements prior to the completion of the two-year term.

82. Before changing its policy concerning data collection and disclosure on October 14, 2011, Verizon Wireless stated that it would provide consumers with "clear and meaningful notice of our practice and obtain [consumers'] affirmative consent" before collecting or disclosing web-browsing information, including internet search terms.[102]

83. Before changing its policy concerning data collection and disclosure on October 14, 2011, Verizon Wireless represented to consumers (through the company's failure to provide notice of collection or disclosure) that the company would not collect or disclose users' location data, demographic information, and mobile device usage information.

84. The company now requires consumers to opt *out* of the companies' collection and disclosure of users' location data, web browsing histories, internet search terms, demographic information, and mobile device usage information. Requiring consumers to opt out is not equivalent to obtaining their *affirmative* consent. Thus, Verizon Wireless deceived consumers about their ability to control access to their personal information.

85. After changing its policy concerning data collection and disclosure on October 14, 2011,Verizon assured consumers that the company "will not [disclose] any information that identifies [the user] personally."[103] But the information that Verizon Wireless collected and disclosed, including geolocation and web address information, personally identifiable. Thus, Verizon Wireless' policy is likely to mislead consumers. Moreover,

---

[99] *Id.*
[100] *Id.*
[101] *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 110 (1984).
[102] Verizon Wireless, *supra*.
[103] *See infra* Appendix A: Important Notice About How Verizon Wireless Uses Information.

consumers acted in reliance on Verizon's representation in selecting the company's services as compared with competing services offered by other providers.

86. Furthermore, mobile phone consumers will likely fail to understand the extent of the personal data disclosure that Verizon Wireless' new policy allows. As FTC Chairman Jon Leibowitz has observed, "consumers don't read privacy policies."[104] And those consumers who do read Verizon Wireless' privacy notice are likely unfamiliar with online data collection and marketing practices.[105] Thus, reasonable consumers are likely to equate a policy declaring that no personally-identifying information will be disclosed with the promise to keep them anonymous.

87. Verizon Wireless's personal data collection and disclosure practices are material. They impact millions of consumers, most of whom are locked into long-term contracts with Verizon Wireless. The company's practices result in the collection and disclosure of voluminous personal information about consumers.

88. Verizon Wireless's description of the effects of opting-out states only that "[consumers] will receive mobile ads whether [they] participate or not," which encourages consumers to forgo their opportunity to opt out, falsely suggesting that users will experience no benefit from opting out.[106]

89. Verizon Wireless continues to engage in the unfair and deceptive data collection and disclosure practices through the date of this complaint.

V. Prayer for Investigation and Relief

90. EPIC urges the Commission to investigate Verizon Wireless, determine the extent of the harm to consumer privacy and safety, require Verizon Wireless to immediately cease its unfair and deceptive data collection and disclosure practices, delete all data collected pursuant to the recent changes, ensure that all data disclosed by Verizon Wireless pursuant to the recent changes is deleted by the recipients; implement an opt-in consent model for all future changes to the company's data collection and disclosure practices, and provide such other relief as the Commission finds necessary and appropriate.

---

[104] U.S. Fed. Trade Comm'n, Introductory Remarks of FTC Chairman Jon Leibowitz at FTC Privacy Roundtable 3 (2009), *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

[105] FTC Deception Policy, *supra* note 93 (noting that the FTC asks "How familiar is the public with the product or service?" in evaluating whether the consumer's interpretation is reasonable); Indeed, a new Carnegie-Mellon study on online advertising found that "many participants have a poor understanding of how Internet advertising works, do not understand the use of first-party cookies, let alone third-party cookies, did not realize that behavioral advertising already takes place, believe that their actions online are completely anonymous unless they are logged into a website, and believe that there are legal protections that prohibit companies from sharing information they collect online." *See* Aleecia M. McDonald and Lorrie Faith Cranor, Carneigie Mellon University, An Empirical Study of How People Perceive Online Behavioral Advertising (Nov. 10, 2009).

[106] *Id.*

91. EPIC reserves the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
John Verdi, EPIC Senior Counsel
David Jacobs, EPIC Consumer Protection Fellow
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

Appendix A: Important Notice About How Verizon Wireless Uses Information

Your privacy is an important priority at Verizon Wireless. View Online

verizon wireless | Explore | Shop | My Verizon | Support

Important notice about how Verizon Wireless uses information.

Why am I getting this notice?	Your privacy is an important priority at Verizon Wireless. Our Privacy Policy (available at www.vzw.com/myprivacy) informs you about information we collect and how we use it. Today we want to tell you about some important updates relating to two new uses of information. Verizon Wireless will begin using the information described below for (1) certain business and marketing reports and (2) making mobile ads you see more relevant. If you do not want us to use this information for these purposes, you can let us know by using one of the options described in the "Your Choices" section of this notice. This supplements our Privacy Policy.
What information are we talking about? Under these programs, we will not share any information that identifies you personally.	Verizon Wireless will use the following categories of information: **Mobile Usage Information:** • Addresses of websites you visit when using our wireless service. These data strings (or URLs) may include search terms you have used • Location of your device ("Location Information") • App and device feature usage **Consumer Information:** • Information about your use of Verizon products and services (such as data and calling features, device type, and amount of use) • Demographic and interest categories provided to us by other companies, such as gender, age range, sports fan, frequent diner, or pet owner ("Demographics")
Is my information shared?	Under these new programs, we will not share outside of Verizon any information that identifies you personally.

HOW INFORMATION WILL BE USED	DESCRIPTION	EXAMPLE
To create business and marketing reports.	We will combine Mobile Usage Information and Consumer Information in a way that does not personally identify you. We will use this information to prepare business and marketing reports that we may use ourselves or share with others.	A report might state that 10,000 mobile users visited a sports website in a month and 60% were men.
For other companies to create business and marketing reports.	We may also share Location Information with other companies in a way that does not personally identify you. We will allow these companies to produce limited business and marketing reports.	The data we provide could be combined with data provided by other wireless carriers to create a report on the number of mobile users who take a particular highway during rush hour.
To make mobile ads you see more relevant.	When you use your wireless device, you often see ads on websites and apps. Using certain Consumer Information (such as your Demographics, device type, and language preference) and the postal address we have for you, we will determine whether you fit within an audience an advertiser is trying to reach. This means ads you see may be more relevant to you. We will not share any information that identifies you personally.	A local restaurant may want to advertise only to people who live within 10 miles, and we might help deliver that ad on a website without sharing information that identifies you personally.

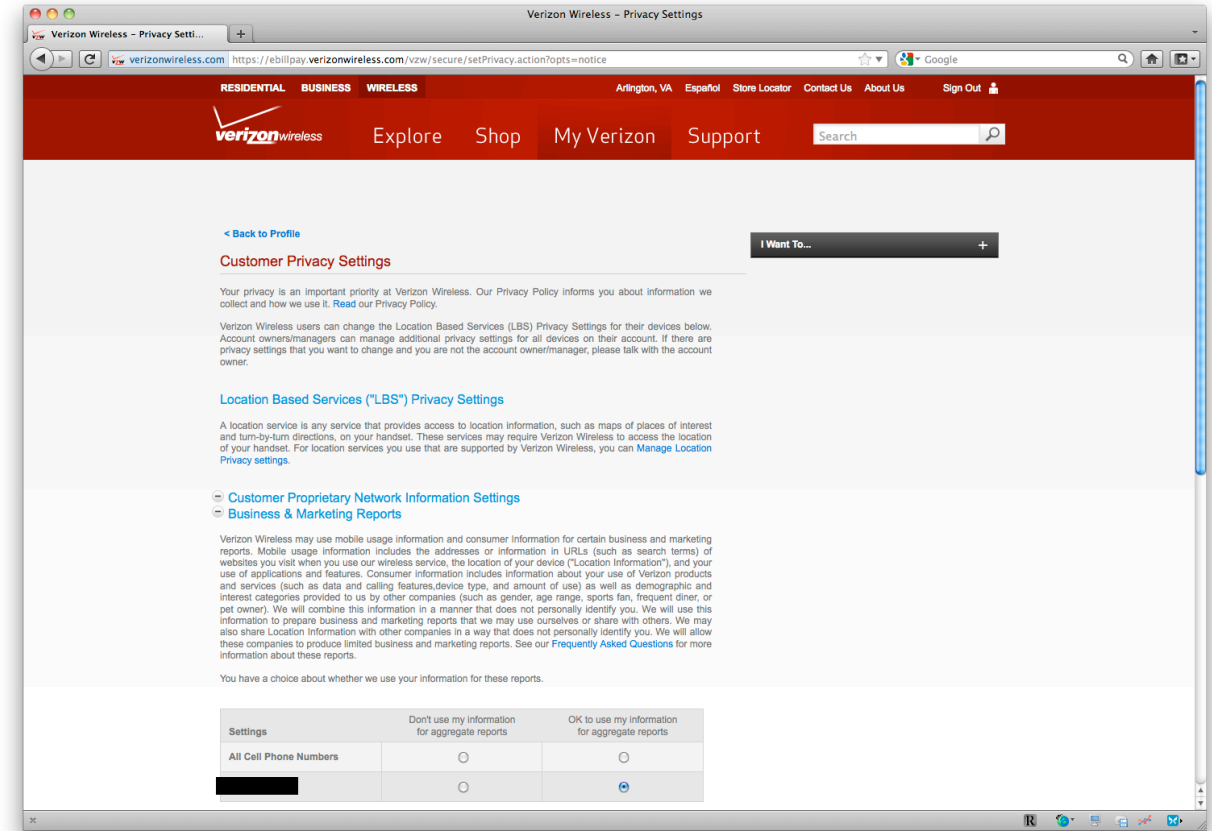
To make mobile ads you see more relevant.	When you use your wireless device, you often see ads on websites and apps. Using certain Consumer Information (such as your Demographics, device type, and language preference) and the postal address we have for you, we will determine whether you fit within an audience an advertiser is trying to reach. This means ads you see may be more relevant to you. We will not share any information that identifies you personally.	A local restaurant may want to advertise only to people who live within 10 miles, and we might help deliver that ad on a website without sharing information that identifies you personally.
Your choices.	**If you do not want us to use your information for any of the purposes described above, please let us know at any time by:** • **Visiting** www.vzw.com/myprivacy **Or** • **Calling** 1-866-211-0874	You will receive mobile ads whether you participate or not, but under the advertising program, ads may be more relevant to you. If you have a Family SharePlan® or multi-line account, you must indicate your choice for each line. If you add a line or change a telephone number, you will need to update your privacy choices.

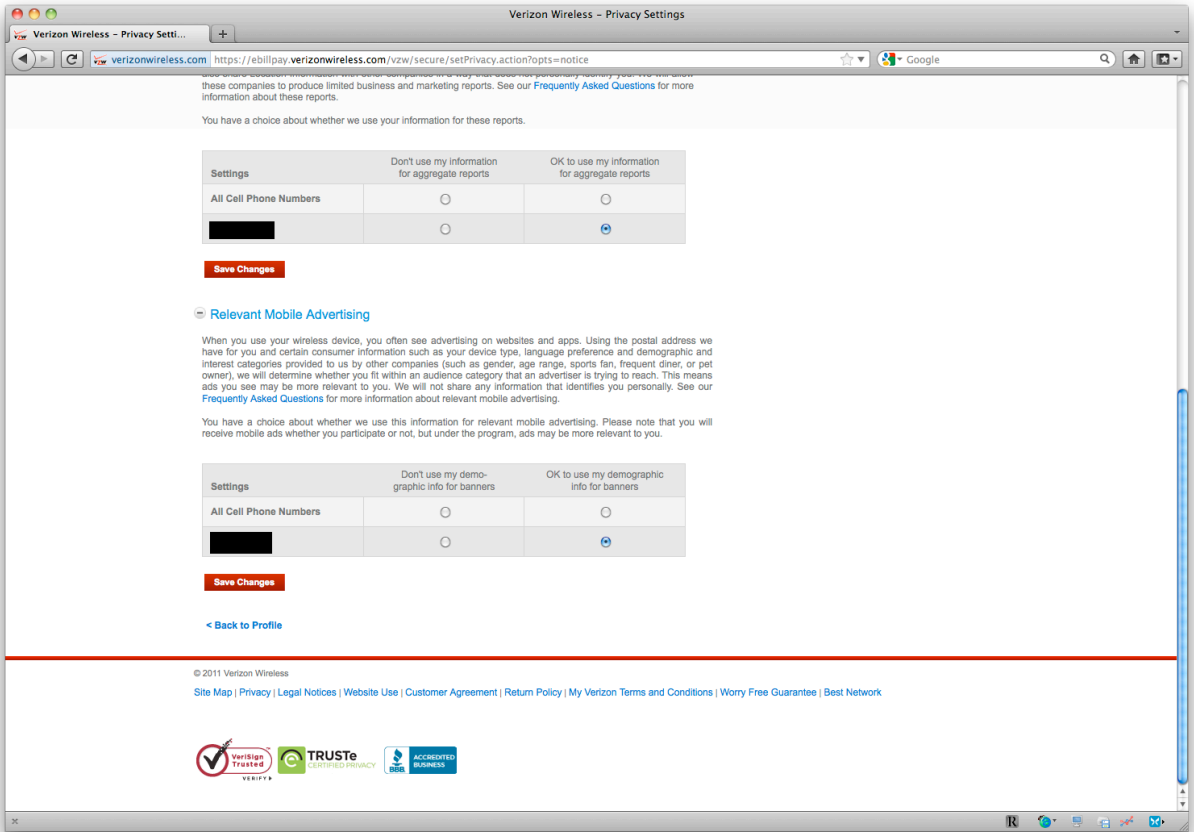
Plans | Phones & Devices | Accessories | Verizon Forums | My Verizon | Retrieve User Name | Retrieve Password

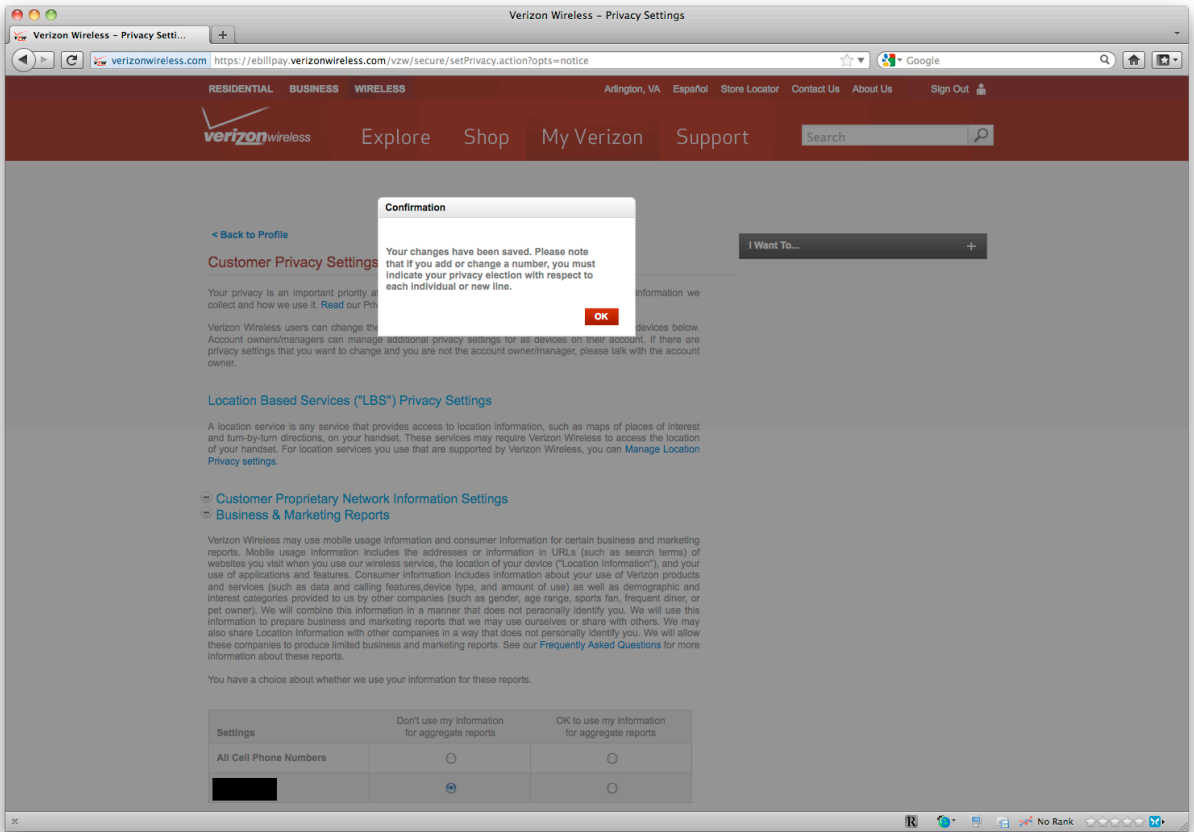
Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

This email was sent to [redacted]
and associated with your Verizon Wireless mobile number ending in 0886.

Appendix B: Customer Privacy Settings




Verizon Wireless – Privacy Settings
Verizon Wireless – Privacy Setti...
verizonwireless.com
https://ebillpay.verizonwireless.com/vzw/secure/setPrivacy.action?opts=notice
Google
these companies to produce limited business and marketing reports. See our Frequently Asked Questions for more information about these reports.
You have a choice about whether we use your information for these reports.
Settings
Don't use my information for aggregate reports
OK to use my information for aggregate reports
All Cell Phone Numbers
[redacted]
Save Changes
Relevant Mobile Advertising
When you use your wireless device, you often see advertising on websites and apps. Using the postal address we have for you and certain consumer information such as your device type, language preference and demographic and interest categories provided to us by other companies (such as gender, age range, sports fan, frequent diner, or pet owner), we will determine whether you fit within an audience category that an advertiser is trying to reach. This means ads you see may be more relevant to you. We will not share any information that identifies you personally. See our Frequently Asked Questions for more information about relevant mobile advertising.
You have a choice about whether we use this information for relevant mobile advertising. Please note that you will receive mobile ads whether you participate or not, but under the program, ads may be more relevant to you.
Settings
Don't use my demo-graphic info for banners
OK to use my demographic info for banners
All Cell Phone Numbers
[redacted]
Save Changes
< Back to Profile
© 2011 Verizon Wireless
Site Map | Privacy | Legal Notices | Website Use | Customer Agreement | Return Policy | My Verizon Terms and Conditions | Worry Free Guarantee | Best Network
VeriSign Trusted
TRUSTe CERTIFIED PRIVACY
ACCREDITED BUSINESS


Verizon Wireless – Privacy Settings
Verizon Wireless – Privacy Setti...
verizonwireless.com
https://ebillpay.verizonwireless.com/vzw/secure/setPrivacy.action?opts=notice
Google
RESIDENTIAL
BUSINESS
WIRELESS
Arlington, VA
Español
Store Locator
Contact Us
About Us
Sign Out
verizonwireless
Explore
Shop
My Verizon
Support
Search
Confirmation
Your changes have been saved. Please note that if you add or change a number, you must indicate your privacy election with respect to each individual or new line.
OK
< Back to Profile
Customer Privacy Settings
I Want To...
Location Based Services ("LBS") Privacy Settings
A location service is any service that provides access to location information, such as maps of places of interest and turn-by-turn directions, on your handset. These services may require Verizon Wireless to access the location of your handset. For location services you use that are supported by Verizon Wireless, you can Manage Location Privacy settings.
Customer Proprietary Network Information Settings
Business & Marketing Reports
Verizon Wireless may use mobile usage information and consumer information for certain business and marketing reports. Mobile usage information includes the addresses or information in URLs (such as search terms) of websites you visit when you use our wireless service, the location of your device ("Location Information"), and your use of applications and features. Consumer information includes information about your use of Verizon products and services (such as data and calling features,device type, and amount of use) as well as demographic and interest categories provided to us by other companies (such as gender, age range, sports fan, frequent diner, or pet owner). We will combine this information in a manner that does not personally identify you. We will use this information to prepare business and marketing reports that we may use ourselves or share with others. We may also share Location Information with other companies in a way that does not personally identify you. We will allow these companies to produce limited business and marketing reports. See our Frequently Asked Questions for more information about these reports.
You have a choice about whether we use your information for these reports.
Settings
Don't use my information for aggregate reports
OK to use my information for aggregate reports
All Cell Phone Numbers
[redacted]
No Rank