Before the
Federal Trade Commission
Washington, DC

In the Matter of	)
	)
Facebook, Inc.	)
	)
	)

Complaint, Request for Investigation, Injunction, and Other Relief

I. Introduction

1. This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. 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.

2. These business practices impact more than 100 million users of the social networking site who fall within the jurisdiction of the United States Federal Trade Commission.[1]

3. EPIC urges the Commission to investigate Facebook, determine the extent of the harm to consumer privacy and safety, require Facebook to restore privacy settings that were previously available as detailed below, require Facebook to give users meaningful control over personal information, and seek appropriate injunctive and compensatory relief.

[1] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009); *see also* Eric Eldon, *Facebook Reaches 100 Million Monthly Active Users in the United States*, InsideFacebook.com, Dec. 7, 2009, http://www.insidefacebook.com/2009/12/07/facebook-reaches-100-million-monthly-active-users-in-the-united-states (last visited Dec. 15, 2009).

II. Parties

4. 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. Among its other activities, EPIC first brought the Commission's attention 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, calling the Commission's attention to "data products circumvent[ing] the FCRA, giving businesses, private investigators, and law enforcement access to data that previously had been subjected to Fair Information Practices."[3] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million.[4] EPIC initiated the complaint to the FTC regarding Microsoft Passport.[5] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[6] EPIC also 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]

---

[2] *In the Matter of DoubleClick*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), *available at* http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[3] *In the Matter of Choicepoint*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Dec. 16, 2004), *available at* http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[4] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress, http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Dec. 13, 2009).

[5] *In the Matter of Microsoft Corporation*, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (July 26, 2001), *available at* http://epic.org/privacy/consumer/MS_complaint.pdf.

[6] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069 (Aug. 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. 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."), *available at* http://www.ftc.gov/opa/2002/08/microst.shtm.

[7] *In the Matter of Awarenesstech.com, et al.*, Complaint and Request for Injunction, Request for Investigation and for Other relief, before the Federal Trade Commission, *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), *available at* http://ftc.gov/os/caselist/0823160/081106cyberspytro.pdf.

5. Earlier this year, EPIC urged the FTC to undertake an investigation of Google and cloud computing.[9] The FTC agreed to review the complaint, stating that it "raises a number of concerns about the privacy and security of information collected from consumers online."[10] More recently, EPIC asked the FTC to investigate the "parental control" software firm Echometrix.[11] Thus far, the FTC has failed to announce any action in this matter, but once the Department of Defense became aware of the privacy and security risks to military families, it removed Echometrix's software from the Army and Air Force Exchange Service, the online shopping portal for military families.[12]

6. The American Library Association is the oldest and largest library association in the world, with more than 64,000 members. Its mission is "to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all."

7. The Center for Digital Democracy ("CDD") is one of the leading non-profit groups analyzing and addressing the impact of digital marketing on privacy and consumer welfare. Based in Washington, D.C., CDD has played a key role promoting policy safeguards for interactive marketing and data collection, including at the FTC and Congress.

8. Consumer Federation of America ("CFA") is an association of some 300 nonprofit consumer organizations across the U.S. CFA was created in 1968 to advance the consumer interest through research, advocacy, and education.

9. Patient Privacy Rights is a non-profit organization located in Austin, Texas. Founded in 2004 by Dr. Deborah Peel, Patient Privacy Rights is dedicated to ensuring Americans control all access to their health records.

10. Privacy Activism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal

---

[9] *In the Matter of Google, Inc., and Cloud Computing Services*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[10] Letter from Eileen Harrington, Acting Director of the FTC Bureau of Consumer Protection, to EPIC (Mar. 18, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

[11] *In the Matter of Echometrix, Inc.*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sep. 25, 2009), *available at* http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.

[12] EPIC, *Excerpts from Echometrix Documents*, http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf (last visited Dec. 13, 2009).

level. A key goal of the organization is to inform the public about the importance of privacy rights and the short- and long-term consequences of losing them, either inadvertently, or by explicitly trading them away for perceived or ill-understood notions of security and convenience.

11. The Privacy Rights Clearinghouse ("PRC") is a nonprofit consumer organization with a two-part mission—consumer information and consumer advocacy. It was established in 1992 and is based in San Diego, CA. Among its several goals, PRC works to raise consumers' awareness of how technology affects personal privacy and to empower consumers to take action to control their own personal information by providing practical tips on privacy protection.

12. The U. S. Bill of Rights Foundation is a non-partisan public interest law policy development and advocacy organization seeking remedies at law and public policy improvements on targeted issues that contravene the Bill of Rights and related Constitutional law. The Foundation implements strategies to combat violations of individual rights and civil liberties through Congressional and legal liaisons, coalition building, message development, project planning & preparation, tactical integration with supporting entities, and the filings of complaints and of *amicus curiae* briefs in litigated matters.

13. Facebook Inc. was founded in 2004 and is based in Palo Alto, California. Facebook's headquarters are located at 156 University Avenue, Suite 300, Palo Alto, CA 94301. At all times material to this complaint, Facebook's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

III. The Importance of Privacy Protection

14. The right of privacy is a personal and fundamental right in the United States.[13] The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.[14]

---

[13] *See Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person"); *Whalen v. Roe*, 429 U.S. 589, 605 (1977); *United States v. Katz*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[14] Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 11 (2009) (charts describing how identity theft victims' information have been misused).

15. The excessive collection of personal data in the United States coupled with inadequate legal and technological protections have led to a dramatic increase in the crime of identity theft.[15]

16. The federal government has established policies for privacy and data collection on federal web sites that acknowledge particular privacy concerns "when uses of web technology can track the activities of users over time and across different web sites" and has discouraged the use of such techniques by federal agencies.[16]

17. As the Supreme Court has made clear, and the Court of Appeals for the District of Columbia Circuit has recently held, "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[17]

18. The Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."

19. The appropriation tort recognizes the right of each person to protect the commercial value of that person's name and likeness. The tort is recognized in virtually every state in the United States.

20. The Madrid Privacy Declaration of November 2009 affirms that privacy is a basic human right, notes that "corporations are acquiring vast amounts of personal data without independent oversight," and highlights the critical role played by "Fair Information Practices that place obligations on those who collect and process personal information and gives rights to those whose personal information is collected."[18]

21. The Federal Trade Commission is "empowered and directed" to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.[19]

---

[15] *Id.* at 5 (from 2000-2009, the number of identity theft complaints received increased from 31,140 to 313,982); *see* U.S. Gen. Accounting Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009); Fed. Trade Comm'n, *Security in Numbers: SSNs and ID Theft* 2 (2008).

[16] Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies* (2000), *available at* http://www.whitehouse.gov/omb/memoranda_m00-13 (last visited Dec. 17, 2009).

[17] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, No. 07-1312 (D.C. Cir. Feb. 13, 2009).

[18] The Madrid Privacy Declaration: Global Privacy Standards for a Global World, Nov. 3, 2009, *available at* http://thepublicvoice.org/madrid-declaration/.

[19] 15 U.S.C. § 45 (2006).

IV. Factual Background

Facebook's Size and Reach Is Unparalleled Among Social Networking Sites

22. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 350 million active users, with more than 100 million in the United States. More than 35 million users update their statuses at least once each day.[20]

23. More than 2.5 billion photos are uploaded to the site each month.[21] Facebook is the largest photo-sharing site on the internet, by a wide margin.[22]

24. As of August 2009, Facebook is the fourth most-visited web site in the world, and the sixth most-visited web site in the United States.[23]

Facebook Has Previously Changed Its Service in Ways that Harm Users' Privacy

25. In September 2006, Facebook disclosed users' personal information, including details relating to their marital and dating status, without their knowledge or consent through its "News Feed" program.[24] Hundreds of thousands of users objected to Facebook's actions.[25] In response, Facebook stated:

> We really messed this one up. When we launched News Feed and Mini-Feed we were trying to provide you with a stream of information about your social world. Instead, we did a bad job of explaining what the new features were and an even worse job of giving you control of them.[26]

26. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program. [27]

27. Facebook is a defendant in multiple federal lawsuits[28] arising from the "Beacon" program.[29] In the lawsuits, users allege violations of federal and state law, including the

---

[20] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009).
[21] *Id*.
[22] Erick Schonfeld, *Facebook Photos Pulls Away From the Pack*, TechCrunch (Feb. 22, 2009), http://www.techcrunch.com/2009/02/22/facebook-photos-pulls-away-from-the-pack/.
[23] Erick Schonfeld, *Facebook is Now the Fourth Largest Site in the World*, TechCrunch (Aug. 4, 2009), http://www.techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world/.
[24] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).
[25] Justin Smith, *Scared students protest Facebook's social dashboard, grappling with rules of attention economy*, Inside Facebook (Sept. 6, 2006), http://www.insidefacebook.com/2006/09/06/scared-students-protest-facebooks-social-dashboard-grappling-with-rules-of-attention-economy/.
[26] Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), http://blog.facebook.com/blog.php?post=2208562130.
[27] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.[30]

28. On May 30, 2008, the Canadian Internet Policy and Public Interest Clinic filed a complaint with Privacy Commissioner of Canada concerning the "unnecessary and non-consensual collection and use of personal information by Facebook."[31]

29. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[32]

30. The Privacy Commissioner's Office found:

> Facebook did not have adequate safeguards in place to prevent unauthorized access by application developers to users' personal information, and furthermore was not doing enough to ensure that meaningful consent was obtained from individuals for the disclosure of their personal information to application developers.[33]

31. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they deleted their accounts.[34] Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising."[35]

32. Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.[36]

---

[28] In *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008), Facebook has requested court approval of a class action settlement that would terminate users' claims, but provide no monetary compensation to users. The court has not ruled on the matter.

[29] *See e.g.*, *Harris v. Facebook, Inc.*, No. 09-01912 (N.D. Tex. filed Oct. 9, 2009); *Lane v. Facebook, Inc.*, No. 5:08-CV-03845 (N.D. Cal. filed Aug. 12, 2008); *see also Harris v. Blockbuster*, No. 09-217 (N.D. Tex. filed Feb. 3, 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).

[30] *Id*.

[31] Letter from Philippa Lawson, Director, Canadian Internet Policy and Public Interest Clinic to Jennifer Stoddart, Privacy Commissioner of Canada (May 30, 2008), *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.

[32] Elizabeth Denham, Assistant Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, July 16, 2009, *available at* http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

[33] *Id*. at 3.

[34] Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."* The Consumerist, Feb. 15, 2009, *available at* http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html#reset.

[35] *Id*.

[36] JR Raphael, *Facebook's Privacy Flap: What Really Went Down, and What's Next*, PC World, Feb. 18, 2009, http://www.pcworld.com/article/159743/facebooks_privacy_flap_what_really_went_down_and_whats_next.html.

Changes in Privacy Settings: "Publicly Available Information"

33. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.[37]

34. Facebook now treats the following categories of personal data as "publicly available information:"

    - users' names,
    - profile photos,
    - lists of friends,
    - pages they are fans of,
    - gender,
    - geographic regions, and
    - networks to which they belong.[38]

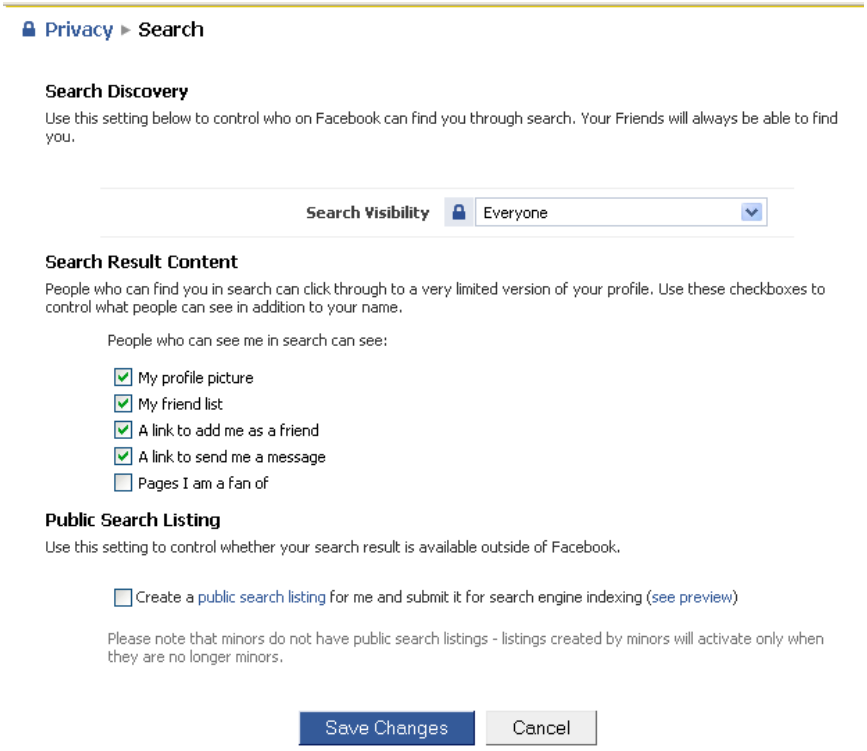
35. By default, Facebook discloses "publicly available information" to search engines, to Internet users whether or not they use Facebook, and others. According to Facebook, such information can be accessed by "every application and website, including those you have not connected with . . . ."[39]

36. Prior to these changes, only the following items were mandatorily "publicly available information:"

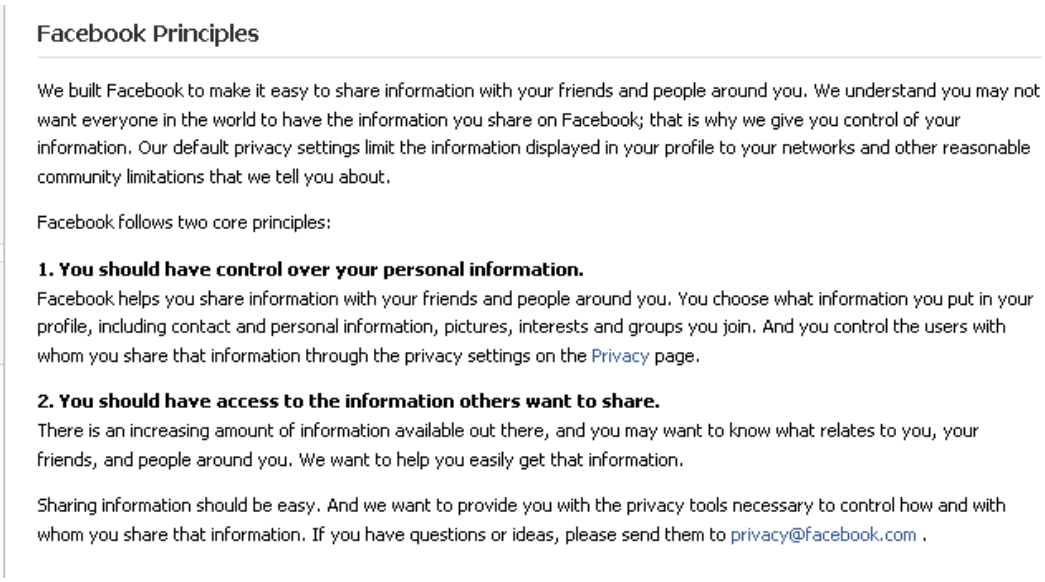
    - a user's name and
    - a user's network.

[37] Facebook, *Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy* (Dec. 9, 2009), *available at* http://www.facebook.com/press/releases.php?p=133917.
[38] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).
[39] *Id.*

37. Users also had the option to include additional information in their public search listing. as the screenshot of the original privacy settings for search discovery demonstrates.



38. Facebook's original privacy policy stated that users "may not want everyone in the world to have the information you share on Facebook" as the screenshot below makes clear:



Facebook Principles

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

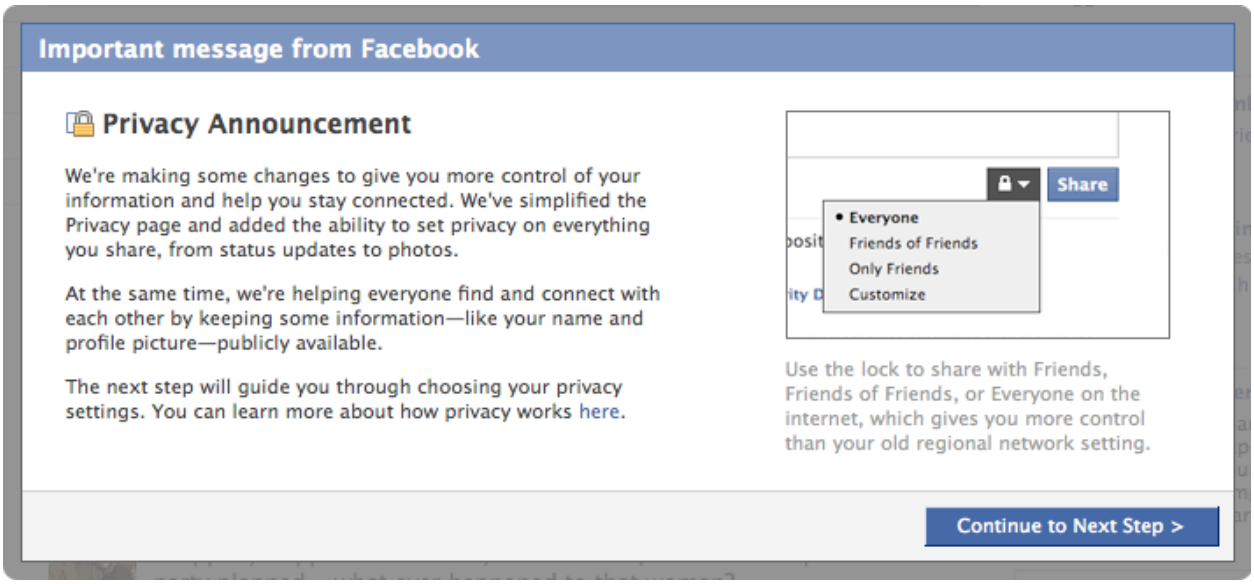
1. You should have control over your personal information.
Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

2. You should have access to the information others want to share.
There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com .

39. Facebook's Chief Privacy Officer, Chris Kelly, testified before Congress that Facebook gives "users controls over how they share their personal information that model real-world information sharing and provide them transparency about how we use their information in advertising."[40] Kelly further testified, "many of our users choose to limit what profile information is available to non-friends. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."[41]

40. In an "Important message from Facebook," Facebook told users it was giving "you more control of your information . . . and [had] added the ability to set privacy on everything you share . . ." as the screen from the transition tool illustrates:



41. Facebook's CEO, Mark Zuckerberg, reversed changes to his personal Facebook privacy settings after the transition from the original privacy settings to the revised settings made public his photographs and other information.[42]

42. Barry Schnitt, Facebook's Director of Corporate Communications and Public Policy, "suggests that users are free to lie about their hometown or take down their profile picture to protect their privacy."[43]

---

[40] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.

[41] *Id.*

[42] Kashmir Hill, *Either Mark Zuckerberg got a whole lot less private or Facebook's CEO doesn't understand the company's new privacy settings* (Dec. 10, 2009), http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/.

43. Providing false information on a Facebook profile violates Facebook's Terms of Service.[44]

44. Facebook user profile information may include sensitive personal information.

45. Facebook users can indicate that they are "fans" of various organizations, individuals, and products, including controversial political causes.[45]

46. Under the original privacy settings, users controlled public access to the causes they supported. Under the revised settings, Facebook has made users' causes "publicly available information," disclosing this data to others and preventing users from exercising control as they had under the original privacy policy.

47. Based on profile data obtained from Facebook users' friends lists, MIT researchers found that "just by looking at a person's online friends, they could predict whether the person was gay."[46] Under Facebook's original privacy policy, Facebook did not categorize users' friends lists as "publicly available information." Facebook now makes users' friends lists "publicly available information."

48. Dozens of American Facebook users, who posted political messages critical of Iran, have reported that Iranian authorities subsequently questioned and detained their relatives.[47] Under the revised privacy settings, Facebook makes such users' friends lists publicly available.

---

[43] Julia Angwin, *How Facebook Is Making Friending Obsolete*, Wall St. J., Dec. 15, 2009, *available at* http://online.wsj.com/article/SB126084637203791583.html.

[44] Facebook, Statement of Rights and Responsibilities, http://www.facebook.com/terms.php (last visited Dec. 16, 2009); *see* Jason Kincaid, *Facebook Suggests You Lie, Break Its Own Terms Of Service To Keep Your Privacy*, Washington Post, Dec. 16, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/15/AR2009121505270.html.

[45] *See, e.g.,* Facebook, *Prop 8*, http://www.facebook.com/pages/Prop-8/86610985605 (last visited Dec. 15, 2009); Facebook, *No on Prop 8 Don't Eliminate Marriage for Anyone*, http://www.facebook.com/#/pages/No-on-Prop-8-Dont-Eliminate-Marriage-for-Anyone/29097894014 (last visited Dec. 15, 2009); *see also Court Tosses Prop. 8 Ruling on Strategy Papers*, San Francisco Chron. (Dec. 12, 2009), *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/12/11/BA3A1B34VC.DTL.

[46] *See* Carolyn Y. Johnson, *Project "Gaydar*," Sep. 20, 2009, Boston Globe, *available at* http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=full

[47] Farnaz Fassihi, *Iranian Crackdown Goes Global*, Wall Street Journal (Dec. 4, 2009), *available at* http://online.wsj.com/article/SB125978649644673331.html.

49. According to the Wall Street Journal, one Iranian-American graduate student received a threatening email that read, "we know your home address in Los Angeles," and directed the user to "stop spreading lies about Iran on Facebook."[48]

50. Another U.S. Facebook user who criticized Iran on Facebook stated that security agents in Tehran located and arrested his father as a result of the postings.[49]

51. One Facebook user who traveled to Iran said that security officials asked him whether he owned a Facebook account, and to verify his answer, they performed a Google search for his name, which revealed his Facebook page. His passport was subsequently confiscated for one month, pending interrogation.[50]

52. Many Iranian Facebook users, out of fear for the safety of their family and friends, changed their last name to "Irani" on their pages so government officials would have a more difficult time targeting them and their loved ones.[51]

53. By implementing the revised privacy settings, Facebook discloses users' sensitive friends lists to the public and exposes users to the analysis employed by Iranian officials against political opponents.

Changes to Privacy Settings: Information Disclosure to Application Developers

54. The Facebook Platform transfers Facebook users' personal data to application developers without users' knowledge or consent.[52]

55. Facebook permits third-party applications to access user information at the moment a user visits an application website. According to Facebook, third party applications receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them."[53]

56. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can

---

[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *See* Facebook, *Facebook Platform*, http://www.facebook.com/facebook#/platform?v=info (last visited Dec. 13, 2009).
[53] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

see.[54] The primary "privacy setting" that Facebook demonstrates to third-party developers governs what other users can see from the application's output, rather than what data may be accessed by the application.[55]

57. According to Facebook:

> Examples of the types of information that applications and websites may have access to include the following information, to the extent visible on Facebook: your name, your profile picture, your gender, your birthday, your hometown location (city/state/country), your current location (city/state/country), your political view, your activities, your interests, your musical preferences, television shows in which you are interested, movies in which you are interested, books in which you are interested, your favorite quotes, your relationship status, your dating interests, your relationship interests, your network affiliations, your education history, your work history, your course information, copies of photos in your photo albums, metadata associated with your photo albums (e.g., time of upload, album name, comments on your photos, etc.), the total number of messages sent and/or received by you, the total number of unread messages in your in-box, the total number of "pokes" you have sent and/or received, the total number of wall posts on your Wall, a list of user IDs mapped to your friends, your social timeline, notifications that you have received from other applications, and events associated with your profile.[56]

58. To access this information, developers use the Facebook Application Programming Interface ("API"), to "utiliz[e] profile, friend, Page, group, photo, and event data."[57] The API is a collection of commands that an application can run on Facebook, including authorization commands, data retrieval commands, and data publishing commands.[58]

---

[54] Facebook, *About Platform*, http://developers.facebook.com/about_platform.php (last visited Dec. 16, 2009).
[55] Facebook Developer Wiki, *Anatomy of a Facebook App*, http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App#Privacy_Settings (last visited Dec. 16, 2009).
[56] Facebook, *About Platform*, http://developers.facebook.com/about_platform.php (last visited Dec. 16, 2009).
[57] Facebook Developer Wiki, *API*, http://wiki.developers.facebook.com/index.php/API (last visited Dec. 16, 2009).
[58] *Id*.

59. Third-parties who develop Facebook applications may also transmit the user information they access to their own servers, and are asked only to retain the information for less than 24 hours.[59]

60. A 2007 University of Virginia study of Facebook applications found that "90.7% of applications are being given more privileges than they need."[60]

61. According to the Washington Post, many Facebook developers who have gained access to information this way have considered the "value" of having the data, even when the data is not relevant to the purpose for which the user has added the application.[61]

62. Under the revised privacy policy, Facebook now categorizes users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong as "publicly available information," and Facebooks sets the "default privacy setting for certain types of information [users] post on Facebook . . . to 'everyone.'"[62]

63. Facebook allows user information that is categorized as publicly available to "everyone" to be: "accessed by everyone on the Internet (including people not logged into Facebook);" made subject to "indexing by third party search engines;" "associated with you outside of Facebook (such as when you visit other sites on the internet);" and "imported and exported by us and others *without* privacy limitations."[63]

64. With the Preferred Developer Program, Facebook will give third-party developers access to a user's primary email address, personal information provided by the user to Facebook to subscribe to the Facebook service, but not necessarily available to the public or to developers.[64] In fact, some users may choose to create a Facebook account precisely to prevent the disclosure of their primary email address.

---

[59] Facebook Developer Wiki, *Policy Examples and Explanations/Data and Privacy*, http://wiki.developers.facebook.com/index.php/Policy_Examples_and_Explanations/Data_and_Privacy (last visited Dec. 16, 2009).

[60] Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs*, http://www.cs.virginia.edu/felt/privacy/ (last visited Dec. 16, 2009).

[61] Kim Hart, *A Flashy Facebook Page, at a Cost to Privacy*, Wash. Post, June 12, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061103759.html

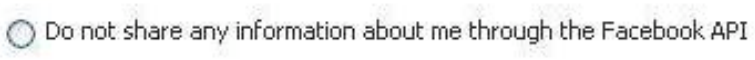
[62] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).

[63] *Id.* (emphasis added)

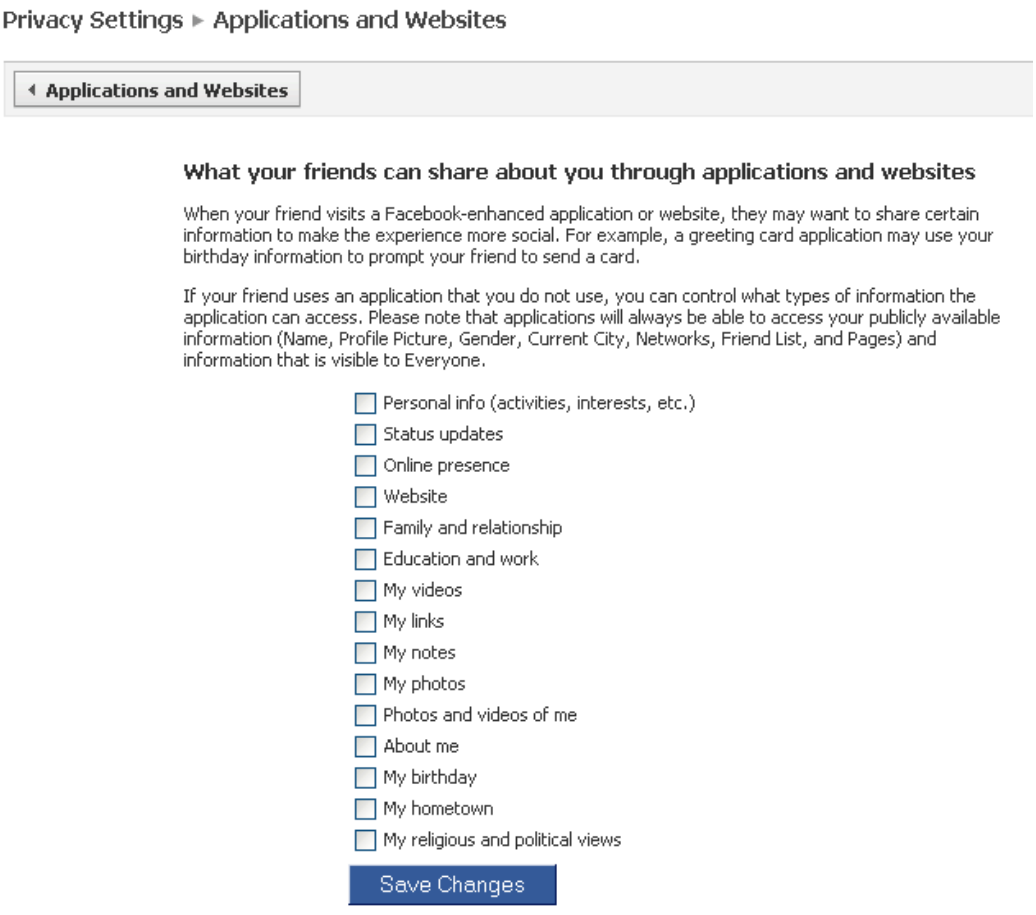
[64] Facebook, *Developer Roadmap*, http://wiki.developers.facebook.com/index.php/Developer_Roadmap (last visited Dec. 17 2009); Facebook, *Roadmap Email*, http://wiki.developers.facebook.com/index.php/Roadmap_Email (last visited Dec. 17, 2009); *see also* Mark Walsh, *Facebook Starts Preferred Developer Program* (Dec. 17, 2009), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=119293.

65. Facebook states in the revised privacy policy that users can "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings."[65] Facebook further states that, "you can control how you share information with those third-party applications and websites through your application settings."[66]

66. In fact, under the original privacy settings, users had a one-click option to prevent the disclosure of personal information to third party application developers through the Facebook API, as the screenshot below indicates:



67. Under the revised privacy settings, Facebook has eliminated the universal one-click option and replaced it with the screen illustrated below:[67]



[65] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).
[66] *Id.*
[67] Facebook, *Privacy Settings*, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share (last visited Dec. 13, 2009).

68. Under the revised settings, even when a user unchecks all boxes and indicates that none of the personal information listed above should be disclosed to third party application developers, Facebook states that "applications will *always* be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone."[68]

69. Facebook's "Everyone" setting overrides the user's choice to limit access by third-party applications and websites.

70. Facebook does not now provide the option that explicitly allows users to opt out of disclosing all information to third parties through the Facebook Platform.

71. Users can block individual third-party applications from obtaining personal information by searching the Application Directory, visiting the application's "about" page, clicking a small link on that page, and then confirming their decision.[69] A user would have to perform these steps for each of more than 350,000 applications in order to block all of them.[70]

Facebook Users Oppose the Changes to the Privacy Settings

72. Facebook users oppose these changes. In only four days, the number of Facebook groups related to privacy settings grew to more than five hundred.[71] Many security experts, bloggers, consumer groups, and news organizations have also opposed these changes.

73. More than 1,050 Facebook users are members of a group entitled "Against The New Facebook Privacy Settings!" The group has a simple request: "We demand that Facebook stop forcing people to reveal things they don't feel comfortable revealing."[72]

74. More than 950 Facebook users are members of a group entitled "Facebook! Fix the Privacy Settings," which exhorts users to "tell Facebook that our personal information is private, and we want to control it!"[73]

---

[68] *Id.* (emphasis added)

[69] Facebook, *General Application Support: Application Safety and Security*, http://www.facebook.com/help.php?page=967 (last visited Dec. 14, 2009).

[70] Facebook, *Statistics*, http://www.facebook.com/press/info.php?statistics (last visited Dec. 14, 2009).

[71] Facebook, *Search "privacy settings,"* http://www.facebook.com/search/?o=69&init=s%3Agroup&q=privacy%20settings (last visited Dec. 15, 2009).

[72] Facebook, *Against The New Facebook Privacy Settings!*, http://www.facebook.com/group.php?gid=209833062912 (last visited Dec. 15, 2009).

75. More than 74,000 Facebook users are members of a group entitled "Petition: Facebook, stop invading my privacy!"[74] The group objects to the revisions and hopes to "get a message across to Facebook."[75] The group description explains, "[o]n December 9, 2009 Facebook once again breached our privacy by imposing new 'privacy settings' on 365+ million users. These settings notably give us LESS privacy than we had before, so I ask, how exactly do they make us more secure? . . . . Perhaps the most frustrating and troublesome part is the changes Facebook made on our behalf without truly making us aware or even asking us."[76]

76. A Facebook blog post discussing the changes to Facebook's privacy policy and settings drew 2,000 comments from users, most of them critical of the changes.[77] One commenter noted, "I came here to communicate with people with whom I have some direct personal connection; not to have my personal information provided to unscrupulous third party vendors and made available to potential stalkers and identity thieves."[78] Another commented, "I liked the old privacy settings better. I felt safer and felt like I had more control."[79]

77. The Electronic Frontier Foundation posted commentary online discussing the "good, the bad, and the ugly" aspects of Facebook's revised privacy policy and settings. More than 400 people have "tweeted" this article to encourage Facebook users to read EFF's analysis.[80]

78. The American Civil Liberties Union of Northern California's Demand Your dotRights campaign started a petition to Facebook demanding that Facebook (1) give full control of user information back to users; (2) give users strong default privacy settings; and (3) restrict the access of third party applications to user data.[81] The ACLU is "concerned that

---

[73] Facebook, *Facebook! Fix the Privacy Settings*, http://www.facebook.com/group.php?gid=192282128398 (last visited Dec. 15, 2009).

[74] Facebook, *Petition: Facebook, stop invading my privacy!*, http://www.facebook.com/group.php?gid=5930262681&ref=share (last visited Dec. 15, 2009).

[75] *Id.*

[76] *Id.*

[77] *See* The Facebook Blog, *Updates on Your New Privacy Tools*, http://blog.facebook.com/blog.php?post=197943902130 (last visited Dec. 14, 2009).

[78] *Id.*

[79] *Id.*

[80] *See* Twitter, *Twitter Search "eff.org Facebook,"* http://twitter.com/#search?q=eff.org%20facebook (last visited Dec. 14, 2009).

[81] American Civil Liberties Union, *Demand Your dotRights: Facebook Petition*, https://secure.aclu.org/site/SPageNavigator/CN_Facebook_Privacy_Petition (last visited Dec. 15, 2009).

the changes Facebook has made actually remove some privacy controls and encourage Facebook users to make other privacy protections disappear."[82]

79. In the past week, more than 3,000 blog posts have been written focusing on criticism of Facebook's privacy changes.[83]

80. After rolling out the revised Facebook privacy settings, widespread user criticism of the change in the "view friends" setting prompted Facebook to roll back the changes in part: "In response to your feedback, we've improved the Friend List visibility option described below. Now when you uncheck the 'Show my friends on my profile' option in the Friends box on your profile, your Friend List won't appear on your profile regardless of whether people are viewing it while logged into Facebook or logged out." Facebook further stated that "this information is still publicly available, however, and can be accessed by applications."[84]

81. Ed Felten, a security expert and Princeton University professor,[85] stated:

> As a user myself, I was pretty unhappy about the recently changed privacy control. I felt that Facebook was trying to trick me into loosening controls on my information. Though the initial letter from Facebook founder Mark Zuckerberg painted the changes as pro-privacy … the actual effect of the company's suggested new policy was to allow more public access to information. Though the company has backtracked on some of the changes, problems remain.[86]

82. Joseph Bonneau, a security expert and University of Cambridge researcher, criticized Facebook's disclosure of users' friend lists, observing,

> there have been many research papers, including a few by me and colleagues in Cambridge, concluding that [friend lists are] actually the most important information to keep private. The threats here are more

---

[82] *Id*; *see also* ACLUNC dotRights, *What Does Facebook's Privacy Transition Mean for You?*, http://dotrights.org/what-does-facebooks-privacy-transition-mean-you (last visited Dec. 16, 2009).
[83] *See* Google, *Google Blog Search "facebook privacy criticism,"* http://blogsearch.google.com/blogsearch?client=news&hl=en&q=facebook+privacy+criticism&ie=UTF-8&as_drrb=q&as_qdr=w (last visited Dec. 14, 2009).
[84] The Facebook Blog, *Updates on Your New Privacy Tools*, http://blog.facebook.com/blog.php?post=197943902130 (last visited Dec. 14, 2009).
[85] Prof. Felton is also Director of the Princeton Center for Information Technology Policy, a cross-disciplinary effort studying digital technologies in public life.
[86] Ed Felten, *Another Privacy Misstep from Facebook* (Dec. 14, 2009), http://www.freedom-to-tinker.com/blog/felten/another-privacy-misstep-facebook.

> fundamental and dangerous-unexpected inference of sensitive information, cross-network de-anonymisation, socially targeted phishing and scams.[87]

Bonneau predicts that Facebook "will likely be completely crawled fairly soon by professional data aggregators, and probably by enterprising researchers soon after."[88]

83. Security expert[89] Graham Cluley stated:

> if you make your information available to "everyone," it actually means "everyone, forever." Because even if you change your mind, it's too late - and although Facebook say they will remove it from your profile they will have no control about how it is used outside of Facebook.

Cluley further states, "there's a real danger that people will go along with Facebook's recommendations without considering carefully the possible consequences."[90]

84. Other industry experts anticipated the problems that would result from the changes in Facebook's privacy settings. In early July, TechCrunch, Jason Kincaid wrote:

> Facebook clearly wants its users to become more comfortable sharing their content across the web, because that's what needs to happen if the site is going to take Twitter head-on with real-time search capabilities Unfortunately that's far easier said than done for the social network, which has for years trumpeted its granular privacy settings as one of its greatest assets. [91]

Kincaid observed that "Facebook sees its redesigned control panel as an opportunity to invite users to start shrugging off their privacy. So it's piggybacking the new 'Everyone' feature on top of the Transition Tool . . ."[92]

---

[87] Joseph Bonneau, *Facebook Tosses Graph Privacy into the Bin* (Dec. 11, 2009), http://www.lightbluetouchpaper.org/2009/12/11/facebook-tosses-graph-privacy-into-the-bin/; *see also* Arvind Narayanan and Vitaly Shmatikov, *De-Anonymizing Social Networks*, *available at* http://www.scribd.com/doc/15021482/DeAnonymizing-Social-Networks-Shmatikov-Narayanan; *Phishing Attacks Using Social Networks*, http://www.indiana.edu/~phishing/social-network-experiment/ (last visited Dec. 15, 2009).

[88] Bonneau, *Facebook Tosses Graph Privacy into the Bin.*

[89] Wikipedia, *Graham Cluley*, http://en.wikipedia.org/wiki/Graham_Cluley.

[90] Graham Cluley, *Facebook privacy settings: What you need to know* (Dec. 10, 2009) http://www.sophos.com/blogs/gc/g/2009/12/10/facebook-privacy/.

[91] Jason Kincaid, *The Looming Facebook Privacy Fiasco* (July 1, 2009), http://www.techcrunch.com/2009/07/01/the-looming-facebook-privacy-fiasco/.

[92] *Id.*

85. Following the changes in Facebook privacy settings, noted blogger Danny Sullivan wrote, "I came close to killing my Facebook account this week." He went on to say, "I was disturbed to discover things I previously had as options were no longer in my control." Sullivan, the editor of Search Engine Land and an expert in search engine design,[93] concluded:

> I don't have time for this. I don't have time to try and figure out the myriad of ways that Facebook may or may not want to use my information. That's why I almost shut down my entire account this week. It would be a hell of a lot easier than this mess.[94]

86. Carleton College librarian Iris Jastram states that the privacy trade-off resulting from the Facebook changes is not "worth it." She writes,

> I'm already making concessions by making myself available to the students who want to friend me there and by grudgingly admitting that I like the rolodex function it plays. But I feel zero motivation to give up more than I can help to Facebook and its third party developers. They can kindly leave me alone, please.[95]

87. Chris Bourg, manager of the Information Center at Stanford University Libraries, notes that "[t]here are some concerns with the new default/recommended privacy settings, which make your updates visible to Everyone, including search engines."[96]

88. Reuters columnist Felix Salmon learned of Facebook's revised privacy settings when Facebook disclosed his "friends" list to critics, who republished the personal information. Salmon apologized to his friends and denounced the Facebook "Everyone" setting:

> I'm a semi-public figure, and although I might not be happy with this kind of cyberstalking, I know I've put myself out there and that there will be consequences of that. But that decision of mine shouldn't have some kind

[93] Wikipedia, *Danny Sullivan (technologist)*, http://en.wikipedia.org/wiki/Danny_Sullivan_(technologist) (last visited Dec. 15, 2009).
[94] Danny Sullivan, *Now Is It Facebook's Microsoft Moment?* (Dec. 11, 2009), http://daggle.com/facebooks-microsoft-moment-1556.
[95] Iris Jastram, *Dear Facebook: Leave Me Alone*, Pegasus Librarian Blog (Dec. 10, 2009), http://pegasuslibrarian.com/2009/12/dear-facebook-leave-me-alone.html.
[96] Chris Bourg, *Overview of new Facebook Privacy Settings*, Feral Librarian (Dec. 9, 2009), http://chrisbourg.wordpress.com/2009/12/09/overview-of-new-facebook-privacy-settings/.

> of transitive property which feeds through to my personal friends, and I don't want the list of their names to be publicly available to everyone.[97]

89. In a blog post responding to the revisions, Marshall Kirkpatrick of ReadWriteWeb wrote, "the company says the move is all about helping users protect their privacy and connect with other people, but the new default option is to change from 'old settings' to becoming visible to 'everyone.' . . . . This is not what Facebook users signed up for. It's not about privacy at all, it's about increasing traffic and the visibility of activity on the site."[98]

90. Jared Newman of PC World details Facebook's privacy revisions.[99] He is particularly critical of the "Everyone" setting:

> By default, Facebook suggests sharing everything on your profile to make it 'easier for friends to find, identify and learn about you.' It should read, 'make it easier for anyone in the world to find, identify and learn about you.' A little creepier, sure, but this is part of Facebook's never-ending struggle to be, essentially, more like Twitter. Thing is, a lot of people like Facebook because it isn't like Twitter. Don't mess with a good thing.[100]

91. Rob Pegoraro blogged on the Washington Post's "Faster Forward" that the Facebook changes were "more of a mess than I'd expected." He criticized the revised "Everyone" privacy setting, stating the change "should never have happened. *Both from a usability and a PR perspective, the correct move would have been to leave users' settings as they were, especially for those who had already switched their options from the older defaults*."[101]

92. In another Washington Post story, Cecilia Kang warned users, "post with care."[102] According to Kang:

> While Facebook users will be able to choose their privacy settings, the problem is that most people don't take the time to do so and may simply

---

[97] Felix Salmon, *Why Can't I Hide My List of Facebook Friends?*, Reuters (Dec. 10, 2009), http://blogs.reutes.com/felix-salmon/2009/12/10/why-cant-i-hide-my-list-of-facebook-friends/.

[98] Marshall Kirkpatrick, ReadWriteWeb, *The Day Has Come: Facebook Pushes People to Go Public*, http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php (last visited Dec. 14, 2009).

[99] http://www.pcworld.com/article/184465/facebook_privacy_changes_the_good_and_the_bad.html

[100] *Id.*

[101] Rob Pegoraro, *Facebook's new default: Sharing updates with 'Everyone'*, Washington Post, Dec. 10, 2009, *available at* http://voices.washingtonpost.com/fasterforward/2009/12/facebook_default_no-privacy.html (emphasis added)

[102] Cecilia Kang, *Facebook adopts new privacy settings to give users more control over content*, Washington Post, Dec. 10, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/09/AR2009120904200.html?hpid=topnews.

> stick with the defaults. Others may find the process confusing and may not understand how to adjust those settings. Facebook said about one in five users currently adjusts privacy settings.[103]

93. New York Times technology writer Brad Stone reported that these changes have not been welcomed by many users.[104] One user wrote:

> It's certainly a violation of my privacy policy. My own 'personal' privacy policy specifically states that I will not share information about my friends with any potential weirdos, child molesters, homicidal maniacs, or anyone I generally don't like.[105]

94. Stone invited readers to comment on their understanding of the changes. Of the more than 50 responses received, most expressed confusion, concern, or anger. One user explained,

> I find the changes to be the exact opposite of what Facebook claims them to be. Things that were once private for me, and for carefully selected Facebook friends, are now open to everyone on the Internet. This is simply not what I signed up for. These are not the privacy settings I agreed to. It is a complete violation of privacy, not the other way around.[106]

95. Another Facebook user wrote,

> There are users like myself that joined Facebook because we were able to connect with friends and family while maintaining our privacy and now FB has taken that away. Im [*sic*] wondering where are the millions of users that told FB it would be a good idea to offer real-time search results of their FB content on Google.[107]

96. A Boston Globe editorial, "Facebook's privacy downgrade," observes that "Facebook's subtle nudges toward greater disclosure coincided with other disconcerting changes: The site is treating more information, such as a user's home city and photo, as 'publicly available information' that the user cannot control. Over time, privacy changes can only

---

[103] *Id.*

[104] Brad Stone, *Facebook's Privacy Changes Draw More Scrutiny*, N.Y. Times, Dec. 10, 2009, *available at* http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny.

[105] *Id.*

[106] *Id.*

[107] Riva Richmond, *The New Facebook Privacy Settings: A How-To*, N.Y. Times, Dec. 11, 2009, *available at* http://gadgetwise.blogs.nytimes.com/2009/12/11/the-new-facebook-privacy-settings-a-how-to/?em.

alienate users." Instead, the Globe argues, "Facebook should be helping its 350 million members keep more of their information private."[108]

97. An editorial from the L.A. Times states simply "what's good for the social networking site isn't necessarily what's good for users."[109]

V. Legal Analysis

The FTC's Section 5 Authority

98. Facebook is engaging in unfair and deceptive acts and practices.[110] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[111] These powers are described in FTC Policy Statements on Deception[112] and Unfairness.[113]

99. 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."[114]

100. The injury must be "substantial."[115] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[116] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[117] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the

---

[108] Editorial, *Facebook's privacy downgrade*, Boston Globe, Dec. 16, 2009, *available at* http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2009/12/16/facebooks_privacy_downgrade.
[109] Editorial, *The business of Facebook*, L.A. Times, Dec. 12, 2009, *available at* http://www.latimes.com/news/opinion/editorials/la-ed-facebook12-2009dec12,0,4419776.story.
[110] *See* 15 U.S.C. § 45.
[111] *Id.*
[112] 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].
[113] 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].
[114] 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.").
[115] FTC Unfairness Policy, *supra* note 113.
[116] *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.").
[117] FTC Unfairness Policy, *supra* note 113.

sales practice also produces."[118] Thus the FTC will not find a practice unfair "unless it is injurious in its net effects."[119] Finally, "the injury must be one which consumers could not reasonably have avoided."[120] 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."[121] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[122]

101. 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."[123] 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."[124]

102. The FTC will make a finding of deception if there has been a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[125]

103. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[126] 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.[127] Second, the act or practice must be considered from the perspective of a reasonable consumer.[128] "The test is whether the consumer's interpretation or reaction is reasonable."[129] 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

[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] FTC Deception Policy, *supra* note 112.
[126] FTC Deception Policy, *supra* note 112; *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).
[127] FTC Deception Policy, *supra* note 112.
[128] *Id.*
[129] *Id.*

omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?"[130]

104. Finally, the representation, omission, or practice must be material.[131] 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.[132] Express claims will be presumed material.[133] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[134] The harms of this social networking site's practices are within the scope of the FTC's authority to enforce Section 5 of the FTC Act and its purveyors should face FTC action for these violations.

Material Changes to Privacy Practices and Misrepresentations of Privacy Policies Constitute Consumer Harm

105. Facebook's actions injure users throughout the United States by invading their privacy; allowing for disclosure and use of information in ways and for purposes other than those consented to or relied upon by such users; causing them to believe falsely that they have full control over the use of their information; and undermining the ability of users to avail themselves of the privacy protections promised by the company.

106. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices, that constitute consumer harm.[135] The Commission realizes the importance of transparency and clarity in privacy policies. "Without real transparency, consumers cannot make informed decisions about how to share their information."[136]

107. The FTC recently found that Sears Holding Management Corporations business practices violated the privacy of its customers.[137] The consent order arose from the company's use of software to collect and disclose users' online activity to third parties,

---

[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] 15 U.S.C. § 45.
[136] Remarks of David C. Vladeck, Director, FTC Bureau of Consumer Protection, New York University: "Promoting Consumer Privacy: Accountability and Transparency in the Modern World" (Oct. 2, 2009).
[137] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

and a misleading privacy policy that did not "adequately [inform consumers as to] the full extent of the information the software tracked."[138] The order requires that the company fully, clearly, and prominently disclose the "types of data the software will monitor, record, or transmit."[139] Further, the company must disclose to consumers whether and how this information will be used by third parties.[140]

108. The Commission has also obtained a consent order against an online company for changing its privacy policy in an unfair and deceptive manner. 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.[141] This was the first enforcement action to "challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[142] Gateway Learning made representations on the site's privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.[143] In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.[144] Gateway then revised its privacy policy to provide for the renting of consumer information "from time to time," applying the policy retroactively.[145] The settlement bars Gateway Learning from, among other things, "misrepresent[ing] in any manner, expressly or by implication . . . the manner in which Respondent will collect, use, or disclose personal information."[146]

109. Furthermore, the FTC has barred deceptive claims about privacy and security policies with respect to personally identifiable, or sensitive, information.[147] In 2008, the FTC issued an order prohibiting Life is Good, Inc. from "misrepresent[ing] in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected

---

[138] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf (last visited Sep. 25, 2009).
[139] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.
[140] *Id.*
[141] Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.
[142] *Id.*
[143] In re Gateway Learning Corp., No. C-4120 (2004) (complaint), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.
[144] *Id.*
[145] *Id.*
[146] In re Gateway Learning Corp., No. C-4120 (2004) (decision and order), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.
[147] In re Life is Good, No. C-4218 (2008) (decision and order), *available at* http://www.ftc.gov/os/caselist/0723046/080418do.pdf.

from or about consumers."[148] The company had represented to its customers, "we are committed to maintaining our customers' privacy," when in fact, it did not have secure or adequate measures of protecting personal information.[149] The Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers' sensitive information.[150]

Facebook's Revisions to the Privacy Settings
Constitute an Unfair and Deceptive Trade Practice

110. Facebook represented that users "may not want everyone in the world to have the information you share on Facebook," and that users "have extensive and precise controls available to choose who sees what among their network and friends, as well as tools that give them the *choice* to make a limited set of information available to search engines and other outside entities."[151]

111. Facebook's changes to users' privacy settings and associated policies in fact categorize as "publicly available information" users' names, profile photos, lists of friends, pages they are fans of, gender, geographic regions, and networks to which they belong.[152] Those categories of user data are no longer subject to users' privacy settings.

112. Facebook represented that its changes to its policy settings and associated policies regarding application developers permit users to "opt-out of Facebook Platform and Facebook Connect altogether through [their] privacy settings,"[153] and tells users, "you can control how you share information with those third-party applications and websites through your application settings"[154]

113. Facebook's changes to users' privacy settings and associated policies regarding application developers in fact eliminate the universal one-click option for opting out of Facebook Platform and Facebook Connect, and replaces it with a less comprehensive

[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] Testimony of Chris Kelly, Chief Privacy Officer, Facebook, Before the U.S. House or Representatives Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection Subcommittee on Communications, Technology and the Internet (June 18, 2009), *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_kelly.pdf.
[152] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 13, 2009).
[153] *Id.*
[154] *Id.*

option that requires users to provide application developers with personal information that users could previously prevent application developers from accessing.[155]

114. Facebook's representations regarding its changes to users' privacy settings and associated policies are misleading and fail to provide users clear and necessary privacy protections.

115. Wide opposition by users, commentators, and advocates to the changes to Facebook's privacy settings and associated policies illustrate that the changes injure Facebook users and harm the public interest.

116. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest.

117. Absent injunctive relief by the Commission, the privacy safeguards for consumers engaging in online commerce and new social network services will be significantly diminished.

VI. Prayer for Investigation and Relief

118. EPIC requests that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, EPIC requests the Commission to:

> Compel Facebook to restore its previous privacy settings allowing users to choose whether to publicly disclose personal information, including name, current city, and friends;
>
> Compel Facebook to restore its previous privacy setting allowing users to fully opt out of revealing information to third-party developers;
>
> Compel Facebook to make its data collection practices clearer and more comprehensible and to give Facebook users meaningful control over personal information provided by Facebook to advertisers and developers; and
>
> Provide such other relief as the Commission finds necessary and appropriate.

[155] Facebook, *Privacy Settings*, http://www.facebook.com/settings/?tab=privacy&section=applications&field=friends_share (last visited Dec. 13, 2009).

119. 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
Kimberly Nguyen, EPIC Consumer Privacy Counsel
Jared Kaprove, EPIC Domestic Surveillance Counsel
Matthew Phillips, EPIC Appellate Advocacy Counsel
Ginger McCall, EPIC National Security Counsel

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

American Library Association
The Center for Digital Democracy
Consumer Federation of America
FoolProof Financial Education
Patient Privacy Rights
Privacy Activism
Privacy Rights Now Coalition
The Privacy Rights Clearinghouse
The U. S. Bill of Rights Foundation

December 17, 2009