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, that adversely impact the users of the service. Facebook now discloses personal information to the public that Facebook users previously restricted. Facebook now discloses personal information to third parties that Facebook users previously did not make 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. The following business practices are unfair and deceptive under Section 5 of the Federal Trade Commission Act: Facebook disclosed users' personal information to Microsoft, Yelp, and Pandora without first obtaining users' consent; Facebook disclosed users' information—including details concerning employment history, education, location, hometown, film preferences, music preferences, and reading preferences—to which users previously restricted access; and Facebook disclosed information to the public even when users elect to make that information available to friends only."

3. These business practices impact more than 115 million users of the social networking site who fall within the jurisdiction of the United States Federal Trade Commission.[1]

[1] *Facebook, Statistics*, http://www.facebook.com/press/info.php?statistics (last visited May 5, 2010); *see also* Inside Facebook, Eric Eldon, *Web Measurement Firms Show Higher Facebook U.S. and World Growth for March 2010*, May 4, 2010, http://www.insidefacebook.com/2010/05/04/web-measurement-firms-show-higher-facebook-us-and-world-growth-for-march-2010/ (last visited May 5, 2010).

4. The Electronic Privacy Information Center, the Bill of Rights Defense Committee, the Center for Digital Democracy, the Center for Financial Privacy and Human Rights, the Center for Media and Democracy, the Consumer Federation of America, the Consumer Task Force for Automotive Issues, Consumer Watchdog, the Foolproof Initiative, Patient Privacy Rights, Privacy Activism, Privacy Journal, the Privacy Rights Clearing House, the United States Bill of Rights Foundation, and U.S. PIRG (hereinafter "Petitioners") urge the Commission to investigate Facebook, determine whether the company has in fact engaged in unfair and/or deceptive trade practices, 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 other appropriate injunctive and compensatory relief.

II. Parties

5. 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.

6. The Bill of Rights Defense Committee ("BORDC") is national, non-partisan, non-profit grassroots advocacy and mobilization network established in 2001 to defend civil rights, civil liberties and rule of law principles eroded by national security policies. The organization organizes and supports a geographically, ethnically, generationally, and ideologically diverse movement around the country by educating people about the significance of those rights in our lives; encouraging widespread civic participation and offering tools to facilitate it; and cultivating and sharing information and opportunities through which Americans from all walks of life can convert their concern into the action needed to restore a constitutional culture uniting our country around rights and values enshrined in the Bill of Rights.

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. The Center for Financial Privacy and Human Rights ("CFPHR"), www.financial.privacy.org, was founded in 2005 to defend privacy, civil liberties and market economics. The Center is a non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy Network, a non-governmental advocacy and research 501(c)(3) organization.

9. The Center for Media and Democracy is an independent, non-profit, non-partisan, public interest organization that focuses on investigating and countering spin by corporations, industry and government; informing and assisting grassroots action that promotes public health, economic justice, ecological sustainability, human rights, and democratic values; advancing transparency and media literacy to help people recognize the forces shaping the information they receive about important issues affecting their lives; and promoting "open content" media that enable people from all walks of life to "be the media" and help write the history of these times.

10. Consumer Federation of America ("CFA") is a non-profit association of nearly 300 non-profit consumer organizations across the United States. Founded in 1968, CFA's mission is to advance consumers' interests through research, education, and advocacy.

11. Consumer Task Force for Automotive Issues ("CTF-A") is a non-profit organization founded by Ralph Nader and Remar Sutton. CTF-A monitors automotive fraud

developments for many Attorneys General, consumer groups, and consumer law firms.

12. Consumer Watchdog was established in 1985 and is a nationally recognized non-partisan, non-profit organization representing the interests of tax payers and consumers. Its mission is to provide an effective voice for the public interest. Consumer Watchdog's programs include health care reform, oversight of insurance rates, energy policy, protecting legal rights, corporate reform, political accountability, and protecting consumer privacy.

13. The Foolproof Initiative is a national organization that teaches young people about consumer advocacy issues.

14. Patient Privacy Rights ("PPR") is the nation's leading health privacy watchdog organization. PPR works to empower individuals and prevent widespread discrimination based on health information using a grassroots, community organizing approach. PPR educates consumers, champions smart policies, and exposes and holds industry and the government accountable. PPR has over 10,000 members in all fifty states. PPR also leads the bipartisan Coalition for Patient Privacy, representing 10 million Americans. The Coalition worked with Congress to ensure that a core of critical consumer security and privacy protections were enacted in the stimulus bill in 2009.

15. Privacy Activism is a non-profit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal 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. www.privacyactivism.com

16. Privacy Journal is the most authoritative publication in the world on the individual's right to privacy. Privacy Journal was founded in 1968 and is published by Robert Ellis Smith, a well-recognized expert on the right to privacy in the United States and author of several essential books on privacy.

17. The Privacy Rights Clearing House ("PRC") is a non-profit, consumer education and advocacy organization based on San Diego, CA and established in 1992. It represents consumers' interests regarding informational privacy at the state and federal levels. Its website provides numerous guides on how to protect personal information. www.privacyrights.org

18. United States 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, mission development, project planning and preparation, tactical integration with other supporting entities, and the filings of *amicus curiae* briefs in litigated matters.

19. U.S. PIRG is an advocate for the public interest. When consumers are cheated, or the voices of ordinary citizens are drowned out by special interest lobbyists, U.S. PIRG speaks up and takes action. U.S.PIRG uncovers threats to public health and well-being and fights to end them, using the time-tested tools of investigative research, media exposés, grassroots organizing, advocacy and litigation. U.S. PIRG's mission is to deliver persistent, result-oriented public interest activism that protects our health, encourages a fair, sustainable economy, and fosters responsive, democratic government.

20. 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

21. The right of privacy is a personal and fundamental right in the United States.[9] 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.[10]

[9] *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).

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

22. 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.[11]

23. 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.[12]

24. 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."[13]

25. 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."

26. 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.

27. 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."[14]

28. According to a Pew Research Center study, most teenage social network users take steps to protect their profiles. Sixty-six percent of teenage social network users

---

[11] *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).

[12] 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).

[13] *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).

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

reported that their profile is not visible to all internet users.[15]They limit access to their profiles in some way. Among those whose profiles can be accessed by anyone online, 46% say they give at least a little and sometimes a good deal of false information on their profiles.[16] Most adult social network users also take measures to protect their profile information.

29. According to a second Pew Research Center study, 60% of adult social network users restrict access to their profiles so that only their friends can see it.[17] Fifty-eight percent of adult social network users restrict access to certain content within their profile.[18]

30. 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]

IV. Factual Background

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

31. Facebook is the largest social network service provider in the United States. According to Facebook, there are more than 400 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]

32. 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]

33. As of March 2010, Facebook is the most-visited web site in the United States.[23]

---

[15] Pew Internet and American Life Project, *Teens, Privacy, and Online Social Networks,* http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx?r=1

[16] *Id.*

[17] Pew Internet and American Life Project, *Social Networks Grow: Friending Mom and Dad*, Jan. 14, 2009, http://pewresearch.org/pubs/1079/social-networks-grow.

[18] *Id.*

[19] 15 U.S.C. § 45 (2006).

[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] Julianne Pepitone, *Facebook Traffic Tops Google for the Week*, Money.cnn.com, March 16, 2010, http://money.cnn.com/2010/03/16/technology/facebook_most_visited/index.htm

34. Faceboook's business practices directly impact more American consumers than any other social network service in the United States.

B. Facebook's has Made User Information "Publicly Available" in Violation of its Privacy Policy

I. Facebook Coverted Facebook Users' Private Information into "Publicly Available" Information

35. During the week of April 18, 2010, Facebook made material changes to the way that a user's personal profile information is classified and disclosed.

36. As a result of these material changes, Facebook requires users to designate personal information as publically linkable "Links," "Pages," or "Connections" or to no longer make such information available.

37. Many Facebook users previously restricted access to this profile data, which includes users' friends list, music preferences, affiliated organizations, employment information, educational institutions, film preferences, reading preferences, and other information.

38. Facebook required users to make these disclosures in several different ways.

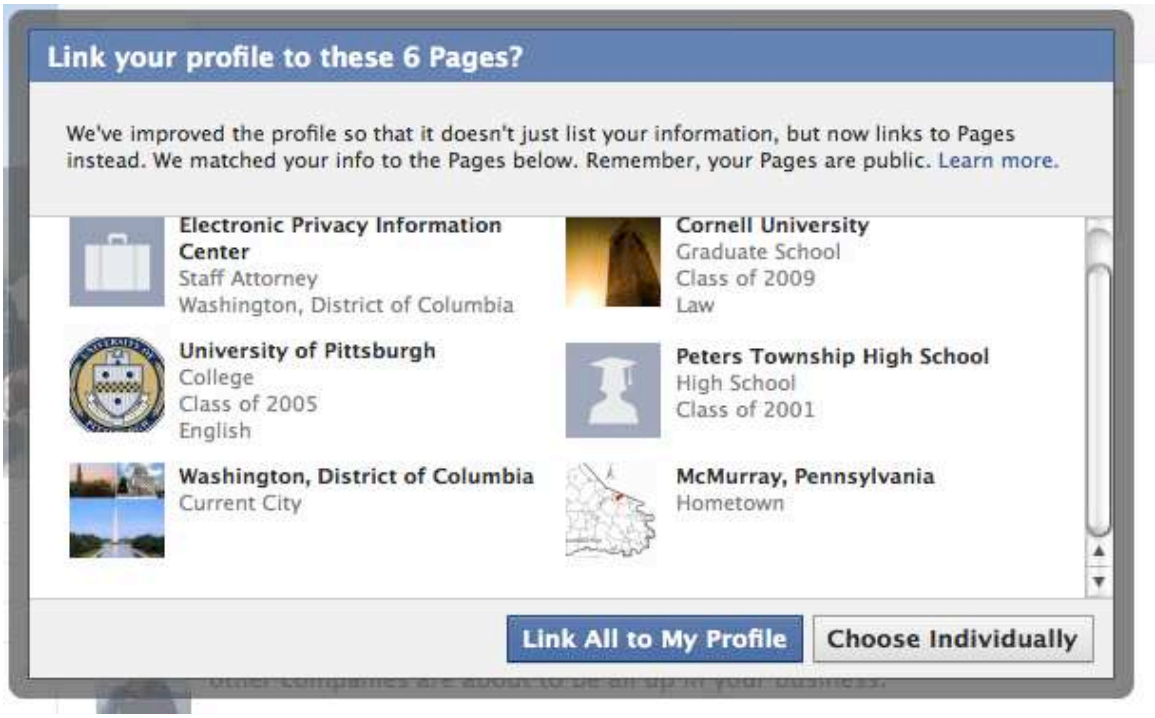
39. Facebook presented some users with a pop-up screen that informed the user that she could "link" her profile to pages that Facebook had selected for her. These pages were selected by Facebook based on existing content in the user's profile, including employer information, education information, and geographic information, as well as music, movie, book, and television preferences.

40. Facebook required users to either "Link All" selected pages to the user's profile, to choose pages individually, or to click "Ask Me Later."

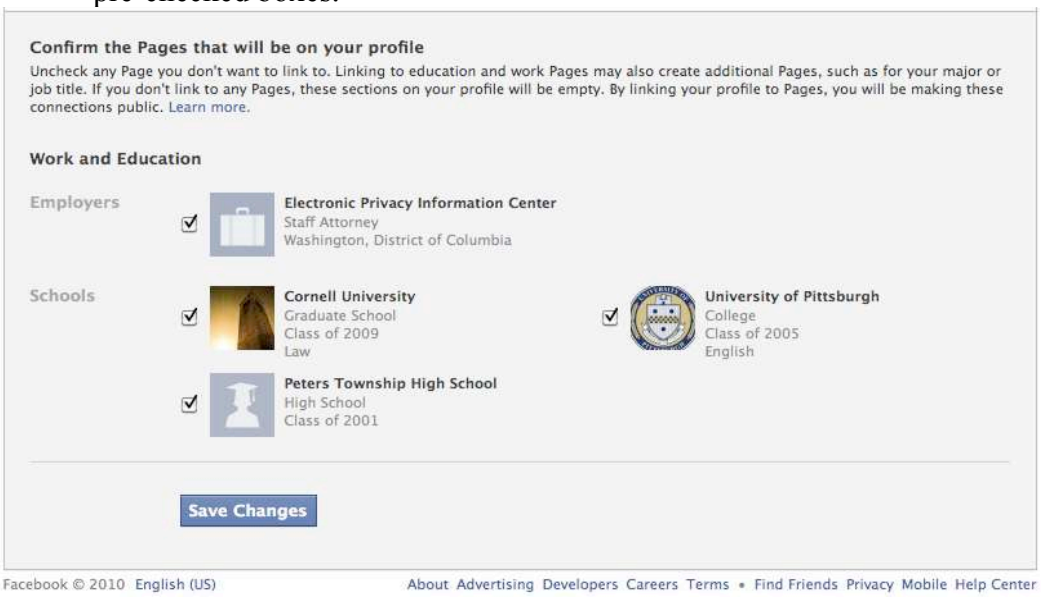
41. If the user selected "Link All" or chose pages individually, the selected pages were added to the user's profile.

42. If the user chose "Ask Me Later," she was allowed to continue to the page to which she was originally navigating.

43. If the user chose "Ask Me Later," the pop-up resurfaced later, this time without the "Ask Me Later" option. This forced the user to select "Link All to My Profile" or "Choose Individually."



44. If the user clicked "Choose Individually," she was taken to a page with a series of pre-checked boxes.



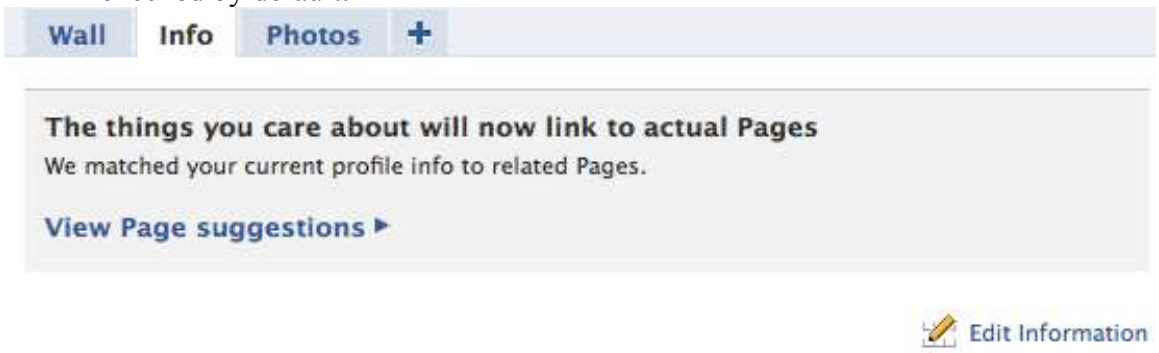
45. If the user unchecked all of the boxes in an attempt to opt-out of the compelled disclosure of her profile information, another pop-up window appeared to inform the user that if no information is designated as "publically available," then major sections of the user's profile that were previously available on the user's Facebook page will be deleted and left empty.

46. As a result of a material changes in its business practice, Facebook no longer permits users to provide "pure text" entries into fields for work and education, current city, hometown, and likes and interests. All entries into these fields must be "linked."

47. Facebook required users to select either "Resume Editing" or "Remove." Resume editing would take the user back to the checked-boxes and offered the user the opportunity to re-check boxes of his choice.

48. If the user chose "Remove," Facebook deleted key pieces of information from the user's profile, such as employment, education, and entertainment preferences, but left the user with a constant reminder that links can be added.

49. Other users were not presented a pop-up window. Instead, Facebook embedded the link announcement in their profile. If the user clicked on "View Page Suggestions" she was taken to the checkbox screen described above – once again, with all links checked by default.



50. Facebook sometimes designates this linkage as a "connection" and other times as a "page." Facebook has designated both connections and pages as publicly viewable information that is no longer protected by users' privacy settings.[24]

51. In the terms under which most Facebook users signed up for the service, employment and educational information and music, film, book, and television preferences were not originally required to be "publicly available" information.[25]

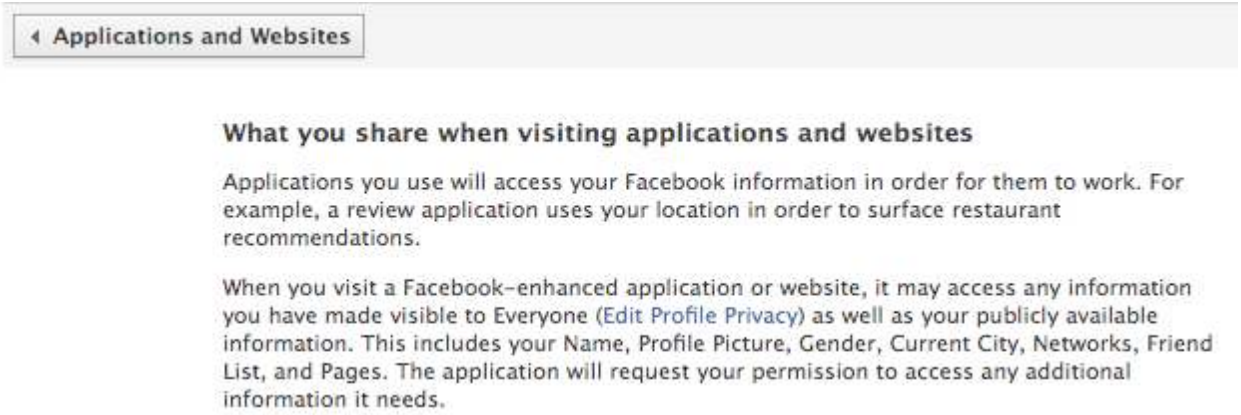
52. After the material changes made by Facebook, a user is now forced to "link" or "connect" personal profile items that were previous protected under the Facebook

[24] Facebook, *Privacy Policy*, www.facebook.com/policy.php (last visited Apr. 27, 2010).
[25] Facebook, *Privacy Policy*, http://web.archive.org/web/20080719134042/http://www.facebook.com/policy.php (dated Dec. 6, 2007).

privacy policy. As a consequence, these items become viewable by everyone. This is because Facebook made these pages "public" that "can be accessed by applications."[26]

53. Facebook states that "if you don't link to any pages, these sections on your profile will be empty. By linking your profile to pages, you will be making these connections public."

54. Facebook states that now websites and applications will have access to "publicly available information. This includes your Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages."[27]



[26] http://www.facebook.com/settings/?tab=privacy&ref=mb#!/settings/?tab=privacy&section=profile_display

[27] http://www.facebook.com/ginger.mccall?ref=profile&v=info#!/settings/?tab=privacy&section=applications&field=learn

55. Thus, Facebook has designated as made "publicly available" information that had previously been protectable under users' privacy settings. This includes information about users' hometown, education, work, activities, likes and interests, and, in some cases, likes and recommendations from non-Facebook pages around the web.

II. Facebook's Privacy Policy is Misleading and Inconsistent with the Site's Representations

56. Facebook's privacy settings and privacy policy are inconsistent with the site's information sharing practices, and Facebook misleads users into believing that users can still maintain control over their personal information.

57. Facebook's current privacy settings allow users to adjust who can see their information, including "Things I Like," "Education and Work," "Friends," "Current City," "Hometown."

58. However, adjustments that users make to their privacy settings only affect what others can see when they navigate to that user's profile page. Facebook obscures the information on the user's profile, but discloses it elsewhere – for instance, on friends' pages, community pages, and to third party websites (including Facebook's connection partners).[28]

59. Facebook discloses information that users designate as available to "Friends Only" to third party websites and applications, as well as other Facebook users, and outsiders who happen upon Facebook Pages or Community Pages.

60. Facebook now designates name, profile picture, gender, current city, hometown, friend list, and pages (including employment and educational information; music, film, television, and book preferences, and current city) as "publicly available" information.

61. Facebook converted some of these categories, including friends list and fan pages, to "publicly available information" after its last round of privacy changes in late 2009.

62. With these most recent changes, Facebook has made new categories of user information, including links, connections, and pages, "publicly available."

63. Facebook's changes require users to put most of their information, including education and employment information; music, film, television, and reading

[28] http://www.facebook.com/ginger.mccall?ref=profile&v=info#!/settings/?tab=privacy&section=profile_display

preferences; and current city, in these "publicly available" categories. Even if a user changes her privacy settings to limit public access to this information, Facebook still discloses the information in places other than the user's profile.

64. The privacy settings are designed to confuse users and to frustrate attempts to limit the public disclosure of personal information that many Facebook users choose to share only with family and friends.

C. "Instant Personalization:" Facebook Discloses the Personal Information of Facebook Users without Consent

I. Social Plugins Violate User Expectations and Reveal User Information Without the User's Consent

65. "Social plugins" are buttons or boxes that appear on third party websites that prompt a Facebook user to click on or comment on items of interest. For example, is a user chooses to "Like" a news article by clicking on a "Like" button, this action is displayed on the third party website, disclosed to the user's friends and appears on the user's Facebook profile.[29]

66. Facebook's Social Plugins may reveal users' personal data to third party websites without clearly indicating to users when their personal information is being given to third party websites.[30]

67. Facebook's Social Plugins include the "like" and "recommend" buttons, activity feed, and recommendations.[31]

68. Facebook represents to users that, "None of your information – your name or profile information, what you like, who your friends are, what they have liked, what they recommend – is shared with the sites you *visit* with a plugin." (emphasis added)[32]

69. However, Facebook permits third party websites that have enabled Facebook's "open graph" to access user information once that user clicks on a Social Plugin application such as the "like" button or "recommend" button. According to Facebook, "When a user establishes this connection by clicking Like on one of your Open Graph –

---

[29] Facebook, Help Center, http://www.facebook.com/help/?page=1068 (last visited May 5, 2010).
[30] *Id.*
[31] Posting of Austin Haugen to The Facebook Blog, *Answers to Your Questions on Personalized Web Tools*, http://blog.facebook.com/blog.php?post=384733792130 (Apr. 26, 2010, 11:17 EST).
[32] Posting of Austin Haugen to The Facebook Blog, *Answers to Your Questions on Personalized Web Tools*, http://blog.facebook.com/blog.php?post=384733792130 (Apr. 26, 2010, 11:17 EST).

enabled pages, you gain the lasting capabilities of Facebook Pages: a link from the user's profile, ability to push the user's News Feed, inclusion in search on Facebook, and analytics through our revamped Insights product."[33]

70. Facebook represents to users that the Like and Recommend "buttons enable you to *publicly* express your interest in some piece of content with a simple action." Facebook further states that by clicking on a Like or Recommend button, a user is "making a *public* connection to it." (emphasis added)[34]

71. Facebook informs users that no information is published if they do not interact (e.g. clicking a Like button) with Social Plugins, and if users do interact with social plugins, Facebook states what information is shared with their friends.[35] However, Facebook fails to tell users what information is disclosed to websites if users interact with social plugins.

72. Although a user is able to control who can see the Connections he makes on his Facebook user profile, Facebook warns users, "Remember that even if you limit the visibility of a connection, it remains as public information and may appear in other places on Facebook.com or be accessed by applications and websites."[36]

73. If a user decides to delete a Social Plugin action, such as liking or recommending a news article, the information will be removed from a user's profile, but will remain visible on third party websites.[37]

II. Instant Personalization Violates User Expectations and Reveals User Information Without the User's Consent

74. Facebook's "Instant Personalization" discloses users' personal information to third party web sites and applications without the users' knowledge or consent.[38]

75. If a user's friend connects with an application or website using Facebook's Instant Personalization, that website will be able to access the user's name, profile picture,

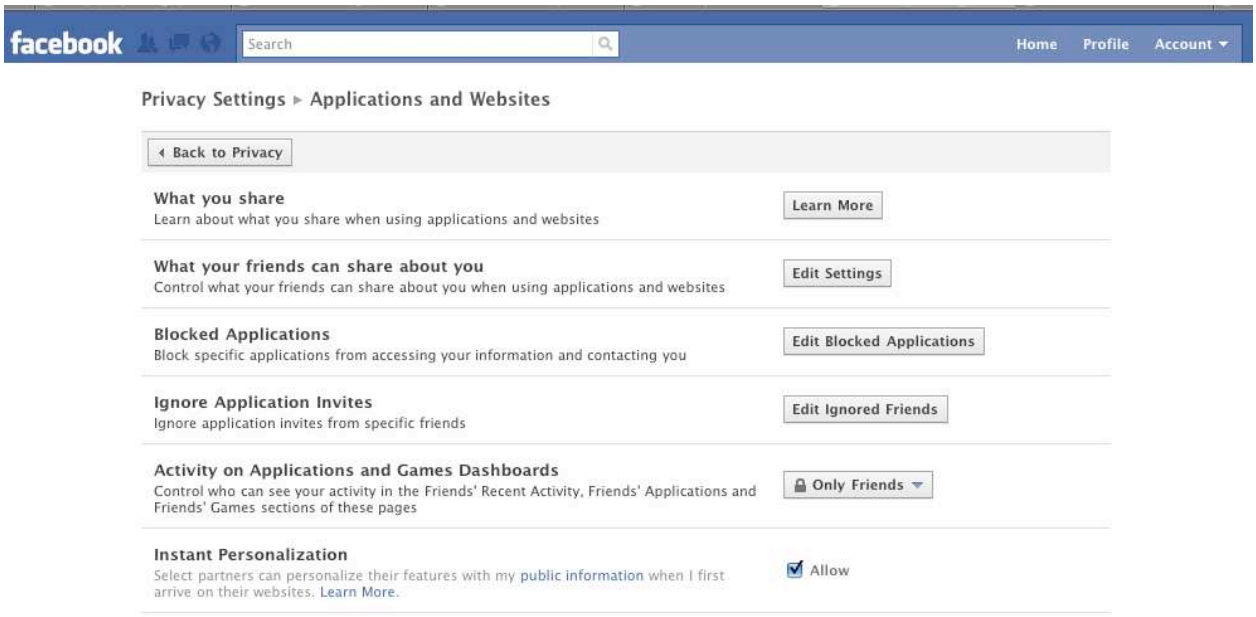
---

[33] Posting of Ethan Beard to Facebook Developers Blog, *A New Data Model*, http://developers.facebook.com/blog/ (Apr. 21, 2010, 16:45 EST).
[34] Facebook, Help Center, http://www.facebook.com/help/?faq=17219 (last visited Apr. 28, 2010).
[35] Facebook, Help Center, *Social plugins and instant personalization*, http://www.facebook.com/help/?page=1068 (last visited Apr. 28, 2010).
[36] Posting of Austin Haugen to The Facebook Blog, *Answers to Your Questions on Personalized Web Tools*, http://blog.facebook.com/blog.php?post=384733792130 (Apr. 26, 2010, 11:17 EST).
[37] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Apr. 26, 2010).
[38] *Id.*

gender, user ID, any connections the user has made, and information the user has shared "everyone."[39]

76. Facebook claims to provide a user with the ability to opt-out, remove pre-approved websites and applications a user has visited, or block pre-approved websites and applications from getting a user's General Information when visited.[40]

77. However, prior to April 23, 2010, Facebook automatically set a user's privacy setting for Instant Personalization as "allow," making it the default, and a user had to deselect this option.



78. Facebook's Help Center section reveals that user information is, by default and without user permission, shared with third party sites.[41]

79. If users disable Instant Personalization, Facebook says that the third parties delete the information that Facebook disclosed.

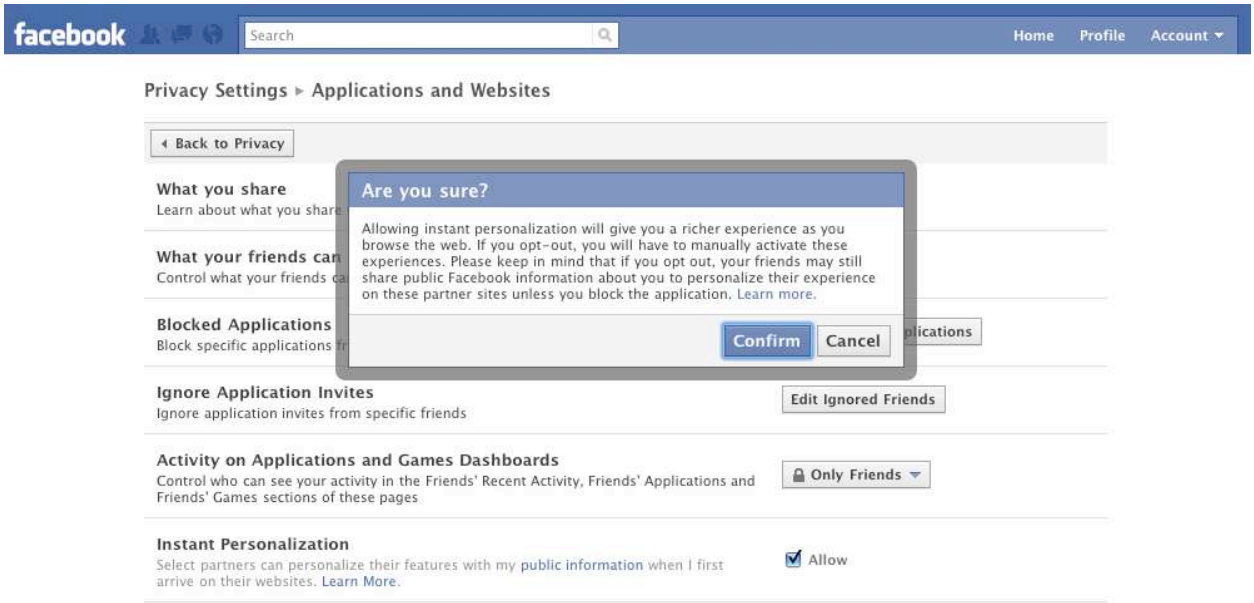
[39] *Id.*
[40] *Id.*
[41] Facebook, Help Center, *Social Plugins and Instant Personalization: How do I opt-out of the instant personalization pilot program,* http://www.facebook.com/help/?page=1068 (last visited May 4, 2010).

How do I opt-out of the instant personalization pilot program?

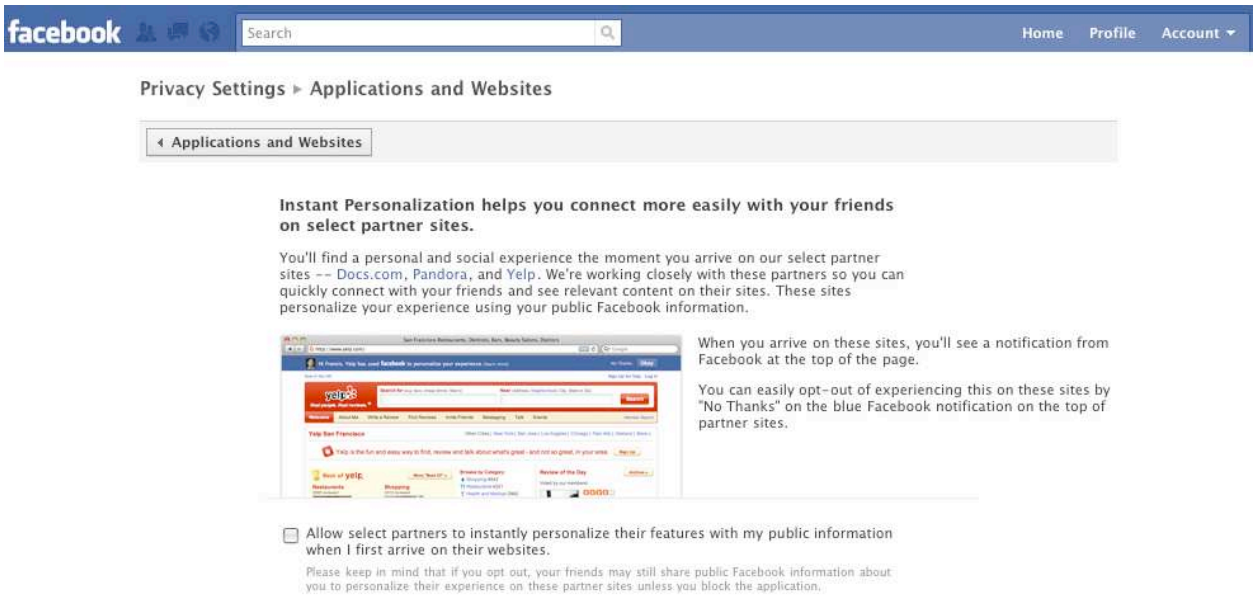
You can opt-out of instant personalization by disallowing it here. By clicking "No Thanks" on the Facebook notification on partner sites, partners will delete your data. To prevent your friends from sharing any of your information with an instant personalization partner, block the application: Microsoft Docs.com, Pandora, Yelp.

http://www.facebook.com/help/?faq=17105

80. Even if a user decides not to allow Instant Personalization, the user's information will be disclosed to third party websites through the user's friends who have not disabled Instant Personalization.



81. After April 23, 2010, Facebook changed the privacy setting for Instant Personalization. A user is now required to check an "allow" box. However, even if a user disables Instant Personalization, Facebook will still disclose this information to third party websites through friends who have not disabled the service.



82. Facebook conceals users' ability to fully disable Instant Personalization. A user is required to go to each individual Facebook Page and click "Block Application" for each Facebook pre-approved website and application before the user's information is protected from distribution to third party websites.

83. Alternatively, Facebook users may go to each individual Facebook pre-approved website or application and select "No Thanks" on the blue Facebook banner that pops down when users visit Instant Personalization websites.

84. Facebook currently discloses users' data *via* Instant Personalization to yelp.com, docs.com, and pandora.com.[42]

85. Facebook has so effectively concealed the process of disabling Instant Personalization that many outside articles have been devoted to guiding users through the process.[43]

86. Facebook's success at concealing the users' option to disable Instant Personalization is evidenced by the fact that many of these outside articles fail to mention the necessity of blocking applications separately.[44]

D. Facebook's Material Changes Limit a Users' Ability to Browse the Internet Anonymously

87. As Facebook seeks to integrate its social network service with third party web sites, Facebook users are no longer able to browse the Internet with relative anonymity.

88. Upon registration, Facebook requires its users to provide their real names, gender, email and birthdates and users are not allowed to provide false personal information and still use Facebook according to the company and its terms of service.[45]

89. Facebook uses cookies to track its users. Thus, whenever a user is logged-in to Facebook and surfing the Internet, he is also transmitting information about which

---

[42] Facebook, Help Center, *Is there a complete list of which websites are enabled for instant personalization?*, http://www.facebook.com/help/?faq=17103 (last visited Apr. 26, 2010).

[43] *See e.g.*, Inventor Spot, Ron Callari, *Opting-Out of Facebook's Instant Personalization,* http://inventorspot.com/articles/opting_out_facebooks_instant_personalization_101_41179

[44] *See e.g.,*Helium, Alicia M. Prater, *How to Opt-Out of Facebook's Instant Personalization,* http://www.helium.com/items/1814046-opt-out-of-facebook-instant-personalization.

[45] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Apr. 26, 2010); Facebook, *Statement of Rights and Responsibilities*, http://www.facebook.com/terms.php (last visited Apr. 26. 2010).

websites he's visited to Facebook. A user does not have to click on or interact with a social plugin for his information trail to be transmitted to Facebook.[46]

90. At Facebook's f8 Conference on April 21, 2010, Facebook 's head of Platform Products, Brett Taylor, stated, "We have the user's cookie. We know who the user is."[47]

91. Facebook's use of cookies is not transparent, and many users are unaware that Facebook is able to track their website viewing practices.

E. Facebook Now Allows Developers to Retain User Data Indefinitely

92. Facebook had previously established a 24-hour data retention time limit for developers that limited the amount of time developers could store/cache user data.[48]

93. Facebook has announced that this limit no longer exists.[49]

94. This allows developers to store user data indefinitely, and is contrary to the terms under which most users agreed to use Facebook.

F. Experts Opposed the Changes to Facebook's Privacy Settings

95. Danny Sullivan, editor-in-chief of Search Engine Land, a blog that covers news and information about search engines and search engine marketing, wrote of the recent changes to the Facebook privacy settings:

> Your product should speak clearly for itself. I shouldn't have to dive into complicated settings that give the fiction of privacy control but don't, since they're so hard to understand that they're ignored. I shouldn't need a flowchart to understand what friends of friends of friends can share with others. Things should be naturally clear and easy for me.[50]

96. Robert Konigsberg, a software engineer at Google, wrote:

---

[46] *Id.*; *see also* Ryan Singel, Today Facebook, Tomorrow the World, Epicenter, Wired (Apr. 23, 2010) http://www.wired.com/epicenter/2010/04/facebook-becomes-web/comment-page-1.

[47], Brett Taylor, Head of Facebook Platform Products, Keynote Address at f8 Conference (Apr. 21, 2010) http://apps.facebook.com/feightlive/ at 18:38.

[48] Posting by Ethan Beard, *supra* note 44.

[49] *Id.*

[50] Danny Sullivan, *Dear Facebook & Google: We Are Not Your Pawns – Enough With The Auto Opt-In!*, Daggle (Apr. 23, 2010) http://daggle.com/dear-facebook-google-pawns-optin-1796.

> Yep! I deactivated my Facebook account today. When Facebook puts me back in control of my data I'll happily return. I'm giving up an easy communications mechanism with my friends, including the one who announced his baby's birth on Facebook, and nowhere else. And I'm walking away. My employer (Google) can't get me to do that. But careless treatment of my personal thoughts and opinions can.[51]

97. Daniel Kusnetzky, a member of the senior management team at The 451 Group stated:

> Facebook constantly is changing the privacy rules and I'm forced to hack through the jungle of their well-hidden privacy controls to prune out new types of permissions Facebook recently added. I have no idea how much of my personal information was released before I learned of a new angle the company has developed to give my information to others.[52]

98. Blake Sabatinelli, online editor/producer for ABC news, reported on Instant Personalization and how it works, stating:

> It could also be a huge step back in privacy, since "Instant Personalization" is turned on automatically by default. That means instead of giving you the option to "opt-in" and give your permission for this to happen, Facebook is making you "opt-out," essentially using your information how they see fit unless you make the extra effort to turn that feature off.[53]

99. Dan Costa, Executive Editor (Reviews) for PCMag Digital Network, wrote:

> Facebook will say that all of this is opt-in, and it is. Hell, no one is making you use Facebook at all…yet. But the truth is no one really understands their own privacy settings now. When Facebook changed its settings six months ago, 65 percent of users chose to keep their profiles public. Or, more likely,

---

[51] Robert Konigsberg, *My issues with Facebook privacy*, Blatherberg (Apr. 25, 2010) http://konigsberg.blogspot.com/2010/04/my-issues-with-facebook-privacy.html.

[52] Daniel Kusnetzky, *Facebook means not being able to control privacy settings*, Virtually Speaking, ZDNet (Apr. 23, 2010) http://blogs.zdnet.com/virtualization/?p=1885.

[53] Blake Sabatinelli, *Facebook's 'Instant Personalization' sparks new round of privacy fears*, ABC Action News, Apr. 23, 2010, http://www.abcactionnews.com/content/news/local/story/how-to-turn-off-facebook-instant-personalization/Oht2YwnnYUqR3Jq8PMwQbw.cspx.

> they just thought they should click "yes" to everything. We have all done it, and that choice will now follow us around the Web—forever.[54]

100. Following the change in Facebook's 24-hour user retention data policy, blogger Sarah Perez wrote a post detaining "How to Delete Facebook Applications (and Why You Should). She highlights that with millions of users, if a popular application's "database was targeted for attack, the payload for hackers could be incredible."[55]

101. In a blog post responding to the recent Facebook changes, Molly Wood of CNet wrote:

> But since Facebook insists on opting me in to these features without my permission, and on opting in all of my friends, and on letting my friends share nearly everything about me *by default* on the sites and applications they use most (on top of everything they want *me* to share), it's pretty obvious that user desires are low on Facebook's priority list. What's high on its list is creating a massive data set that can be sliced, diced, and monetized until the cows come home.[56]

102. Christian Science Monitor writer Matthew Shaer reported on Facebook's social plug-ins, and elicited comments from Facebook users asking whether they were onboard with the changes or opposed to them.[57] Of the more than 40 comments received, most expressed frustration, anger and opposition. One user wrote:

> The fact that I was "opted in" is really my problem. I do not like going to Yelp and seeing what my friends have been yelping. While my yelp/pandora use is pretty tame, I still don't want it going past *MY* computer screen. More to the point, it has gotten to the point where using facebook has felt like a job. I plan on deleting my account as soon as I am done writing this."[58]

---

[54] Dan Costa, *Facebook: Privacy Enemy Number One?*, PCMag.com, Apr. 22, 2010, http://www.pcmag.com/article2/0,2817,2362967,00.asp?kc=PCRSS03079TX1K0000585.

[55] Sarah Perez, *How to Delete Facebook Applications (and Why You Should)*, ReadWriteWeb (Apr. 22, 2010) http://www.readwriteweb.com/archives/how_to_delete_facebook_applications_and_why_you_should.php.

[56] Molly Wood, *How Facebook is putting its users last*, CNet (Apr. 23, 2010) http://news.cnet.com/8301-31322_3-20003185-256.html.

[57] Matthew Shaer, *How long before Facebook users revolt against the latest update?*, The Christian Science Monitor, April 23, 2010, *available at* http://www.csmonitor.com/Innovation/Horizons/2010/0423/How-long-before-Facebook-users-revolt-against-the-latest-update.

[58] *Id.*

103. Another user wrote, "Nothing about this site is private any longer no matter what settings you choose. I deleted all content, unliked everything I could find as far back as I could and deactivated my account. I am not for sale."[59]

104. Christina Warren of Mashable.com, a social media news blog, warned Facebook users to "Be aware of your privacy settings. She pointed out that with Facebook's changes, privacy has become the user's responsibility, stating:

> Public no longer means "public on Facebook," it means "public in the Facebook ecosystem." Some companies, like Pandora, are going to go to great lengths to allow users to separate or opt out of linking their Pandora and Facebook accounts together, but users can't expect all apps and sites to take that approach. My advice to you: Be aware of your privacy settings."[60]

105. Commenting on Facebook's changes, Maurice Cacho of MSN Tech & Gadgets, wrote:

> But this is just another example how there is no real privacy on the web. The latest chapter added to Facebook's growth is just exposing another cloak of privacy before it's picked away at the edges and stripped off your forehead, exposing your inner thoughts to the world as the Internet becomes more of a global playground.[61]

106. Irene North of the Daily Censored, wrote:

> Facebook has become Big Brother. Facebook has succeeded in giving its users the allusion of privacy on a public site, leaving everyone to become complacent about keeping track of the myriad changes going on behind the scenes. The constant changes assure Facebook that you can never keep all your information private.[62]

107. It is clear that Facebook has not made it easy for users to opt out of Instant Personalization or informed users about how social plugins work and how user data is disseminated to third party websites because numerous news outlets and bloggers

---

[59] *Id.*

[60] Christina Warren, *Facebook Open Graph: What it Means for Privacy*, Mashable (Apr. 21, 2010) http://mashable.com/2010/04/21/open-graph-privacy/.

[61] Maurice Cacho, *Toss out your privacy as Facebook becomes more stalker-ish*, MSN Tech & Gadgets (Apr. 21, 2010) http://www.geektown.ca/2010/04/toss-out-your-privacy-as-facebook-becomes-more-stalkerish.html.

[62] Irene North, *People concerned over more Facebook privacy changes*, The Daily Censored (Apr. 26, 2010) http://dailycensored.com/2010/04/26/people-concerned-over-more-facebook-privacy-changes/.

have expressed frustration and concern and found it necessary to write guides to help users to become better informed.[63]

108. After receiving "many questions" from Facebook users about social plugins and Instant Personalization, Facebook product manager Austin Haugen posted an entry on The Facebook Blog entitled, "Answers to Your Questions on Personalized Web Tools," on April 26, 2010.[64]

G. Facebook Users Oppose the Facebook Changes to the Privacy Settings

109. Facebook users oppose these changes. Several new Facebook groups have sprung up in the wake of the changes, and older privacy themed groups have also expressed opposition.

110. More than 840 users are members of a group called "Make Instant Personalization Opt-In," which states "Facebook just rolled out another scheme for sharing personal information about its users with external web sites on an opt-out basis. Even worse, opting out doesn't even prevent that information being shared, should your friends feel like doing so (will they even know they are?), unless you block each application separately."[65]

111. More than 2,278,100 users are members of a group called, "Millions Against Facebook's Privacy Policies and Layout Redesign." The group keeps users up to date

---

[63] Kristin Burnham, *Facebook Privacy Changes: 5 Can't-Miss Facts*, CIO, Apr. 23, 2010, *available at* http://www.cio.com/article/591831/Facebook_Privacy_Changes_5_Can_t_Miss_Facts; Gina Trapani, *Time to Audit Your Facebook Privacy Settings, Here's How*, Fast Company Magazine, Apr. 23, 2010, *available at* http://www.fastcompany.com/1624745/time-to-audit-your-facebook-privacy-settings; Mathew Ingram, *Your Mom's Guide to Those Facebook Changes, and How to Block Them*, Gigaom (Apr. 22, 2010), http://gigaom.com/2010/04/22/your-moms-guide-to-those-facebook-changes-and-how-to-block-them/; Kurt Opshal, *How to Opt Out of Facebook's Instant Personalization*, Deeplinks Blog, (Apr. 22, 2010), http://w2.eff.org/deeplinks/2010/04/how-opt-out-facebook-s-instant-personalization/; Rob Pegoraro, *As Facebook users fret over its wider reach, Post readies opt-out*, Faster Forward, The Washington Post (Apr. 23, 2010), http://voices.washingtonpost.com/fasterforward/2010/04/facebook_users_fret_over_its_w.html; Riva Richmond, *How to Opt Out of Facebook's Instant Personalization*, Gadgetwise Blog, The New York Times (Apr. 23, 2010), http://gadgetwise.blogs.nytimes.com/2010/04/23/how-to-opt-out-of-facebooks-instant-personalization/.

[64] Posting of Austin Haugen to The Facebook Blog, *Answers to Your Questions on Personalized Web Tools*, http://blog.facebook.com/blog.php?post=384733792130 (Apr. 26, 2010, 11:17 EST).

[65] Facebook, *Make Instant Personalization Opt-In*, http://www.facebook.com/group.php?gid=115708625123121&v=info (last visited May 3, 2010).

on Facebook's frequent privacy policy changes and attempts to inform users on how to protect their personal information.[66]

112. More than 950 users "Like" a page called, "I hate the new facebook privacy settings," informing users that "Facebook just changed the privacy options and it's pretty annoying because now almost everything is visible to people we don't know…so LIKE if you agree with me."[67]

113. Over 1,205 users "Like" a group called "Our privacy matters right here!," protesting against the new privacy settings and the lack of user control over personal information.[68]

114. More than 3,470 users are members of a group called, "Facebook! Fix the Privacy Settings," which exhorts users to "Tell Facebook that our personal information is private, and we want to control it!"[69]

115. MoveOn.org, a family of organizations including a non-profit and a federal PAC, began circulating a petition against Facebook stating, "Facebook must respect my privacy. They should not tell my friends what I buy on other sites – or let companies use my name to endorse their products – without my permission."[70]

116. MoveOn.org also hosts a Facebook group called, "Petition: Facebook, stop invading my privacy!" with over 72,685 members demanding that their privacy be respected.[71]

117. A Facebook blog post discussing the changes to Facebook's Privacy Policy and Statement of Rights and Responsibilities elicited numerous comments from users, most of them critical of the changes. One commenter noted, "DISLIKE! Completely horrified and disgusted by your recent changes, and the way you make it a giant pain

---

[66] Facebook, *Millions Against Facebook's Privacy Policies and Layout Redesign*, http://www.facebook.com/group.php?gid=27233634858&v=info (last visited May 3 2010).

[67] Facebook, *I hate the new facebook privacy settings*, http://www.facebook.com/pages/I-hate-the-new-facebook-privacy-settings/246372636176 (last visited May 3, 2010).

[68] Facebook, *Our privacy matters right here!*, http://www.facebook.com/ourprivacymatters (last visited May 3, 2010).

[69] Facebook, *Facebook! Fix the Privacy Settings*, http://www.facebook.com/group.php?gid=192282128398 (last visited May 3, 2010).

[70] MoveOn.org, *Facebook must respect privacy*, http://civ.moveon.org/facebookprivacy/071120email.html (last visited Apr. 29, 2010).

[71] Facebook, *Petition: Facebook, stop invading my privacy!*, http://www.facebook.com/group.php?gid=5930262681 (last visited May 3, 2010).

to opt out of your stupid data-mining/marketing project."[72] Another commented, "HATE that you guys link my profile to everyone WITHOUT my say so. I was STALKED in 1998 and try to keep a low profile by locking out everyone except my friends."[73]

118. The Electronic Frontier Foundation posted commentary online giving Facebook users a step-by-step on how to opt-out of Facebook's Instant Personalization.[74]

119. In response to Facebook's recent changes, Senators Charles Schumer, Michael Bennet, Mark Begich and Al Fraken have asked the FTC to design privacy rules for social networking sites like Facebook, MySpace and Twitter, including guidelines for how user information is used and disseminated.[75]

120. A survey conducted by Sophos, an IT security company, showed that 95% of the 680 Facebook users polled opposed the privacy changes Facebook proposed in March 2010 to allow for social plug-ins and Instant Personalization.[76]

H. Facebook Has a History of Changing Its Service in Ways that Harm Users' Privacy

121. 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.[77] Hundreds of thousands of users objected to Facebook's actions.[78] In response, Facebook stated:

---

[72] Facebook Site Governance, http://www.facebook.com/fbsitegovernance?v=wall&story_fbid=120701477944064 (Apr. 25, 2010, 17:57 EST).

[73] *Id.*

[74] Kurt Opsahl, *How to Opt Out of Facebook's Instant Personalization*, Deeplink Blog (Apr. 22, 2010), http://w2.eff.org/deeplinks/2010/04/how-opt-out-facebook-s-instant-personalization/.

[75] Press Release, Senator Charles E. Schumer, Schumer: Decision by Facebook to Share Users' Private Information with Third-Party Websites Raises Major Privacy Concerns; Calls on FTC to Put in Place Guidelines for Use of Private Information and Prohibit Access Without User Permission (Apr. 26, 2010) http://schumer.senate.gov/record.cfm?id=324175&. *See also*, Michael Liedtke, *Senators see privacy problem in Faccebook expansion*, The Sydney Morning Herald, Apr. 27, 2010, *available at* http://news.smh.com.au/breaking-news-technology/senators-see-privacy-problem-in-facebook-expansion-20100427-tprc.html.

[76] Sophos, *95% of Facebook users oppose privacy policy changes, Sophos poll reveals* (Apr. 7, 2010), http://www.sophos.com/pressoffice/news/articles/2010/04/facebook-poll.html.

[77] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

[78] 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/.

> 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.[79]

122. In 2007, Facebook disclosed users' personal information, including their online purchases and video rentals, without their knowledge or consent through its "Beacon" program. [80]

123. Facebook is a defendant in multiple federal lawsuits[81] arising from the "Beacon" program.[82] In the lawsuits, users allege violations of federal and state law, including the Video Privacy Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Computer Crime Law.[83]

124. 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."[84]

125. On July 16, 2009, the Privacy Commissioner's Office found Facebook "in contravention" of Canada's Personal Information Protection and Electronic Documents Act.[85]

126. On February 4, 2009, Facebook revised its Terms of Service, asserting broad, permanent, and retroactive rights to users' personal information—even after they

---

[79] Mark Zuckerberg, *An Open Letter from Mark Zuckerberg* (Sept. 8, 2006), http://blog.facebook.com/blog.php?post=2208562130.

[80] *See generally* EPIC, *Facebook Privacy*, http://epic.org/privacy/facebook/ (last visited Dec. 15, 2009).

[81] 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.

[82] *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).

[83] *Id*.

[84] 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.

[85] 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.

deleted their accounts.[86] Facebook stated that it could make public a user's "name, likeness and image for any purpose, including commercial or advertising."[87] Users objected to Facebook's actions, and Facebook reversed the revisions on the eve of an EPIC complaint to the Commission.[88]

127. Facebook updated its privacy policy and changed the privacy settings available to users on November 19, 2009 and again on December 9, 2009.[89]

128. Facebook made the following categories of personal data "publicly available information:"

- users' names,
- profile photos,
- lists of friends,
- pages they are fans of,
- gender,
- geographic regions, and
- networks to which they belong.[90]

129. 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 . . . ."[91]

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

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

[86] 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.
[87] *Id*.
[88] 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.
[89] 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.
[90] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 16, 2009).
[91] *Id.*

131. EPIC and a broad coalition of organizations filed a complaint with the FTC in December 2009 regarding these changes.

132. Millions of users joined online groups and campaigns challenging Facebook's changes.

V. Legal Analysis

A. The FTC's Section 5 Authority

133. Facebook is engaging in unfair and deceptive acts and practices.[92] Such practices are prohibited by the FTC Act, and the Commission is empowered to enforce the Act's prohibitions.[93] These powers are described in FTC Policy Statements on Deception[94] and Unfairness.[95]

134. 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."[96]

135. The injury must be "substantial."[97] Typically, this involves monetary harm, but may also include "unwarranted health and safety risks."[98] Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[99] Secondly, the injury "must not be outweighed by an offsetting consumer or competitive benefit that the sales practice also produces."[100] Thus the FTC will not find a practice unfair

---

[92] *See* 15 U.S.C. § 45.
[93] *Id.*
[94] 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].
[95] 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].
[96] 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.").
[97] FTC Unfairness Policy, *supra* note 113.
[98] *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.").
[99] FTC Unfairness Policy, *supra* note 113.
[100] *Id.*

"unless it is injurious in its net effects."[101] Finally, "the injury must be one which consumers could not reasonably have avoided."[102] 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."[103] Sellers may not withhold from consumers important price or performance information, engage in coercion, or unduly influence highly susceptible classes of consumers.[104]

136. 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."[105] 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."[106]

137. 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."[107]

138. First, there must be a representation, omission, or practice that is likely to mislead the consumer.[108] 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.[109] Second, the act or practice must be considered from the perspective of a reasonable consumer.[110] "The test is whether the consumer's interpretation or reaction is reasonable."[111] 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?"[112]

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] FTC Deception Policy, *supra* note 112.
[108] 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).
[109] FTC Deception Policy, *supra* note 112.
[110] *Id.*
[111] *Id.*
[112] *Id.*

139. Finally, the representation, omission, or practice must be material.[113] 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.[114] Express claims will be presumed material.[115] Materiality is presumed for claims and omissions involving "health, safety, or other areas with which the reasonable consumer would be concerned."[116] 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.

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

140. 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.

141. The FTC Act empowers and directs the FTC to investigate business practices, including data collection practices that constitute consumer harm.[117] 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."[118]

142. In 2002, the FTC settled a privacy enforcement action against Microsoft for violations associated with the Microsoft Passport identification and authentication system that collected users' personal information in connection with making purchases.[119] The settlement arose from the company's false representations about how personal information was protected, the security of making purchases through the Passport system, not collecting any personally identifiable information other than that described in the privacy policy, and that parents had control over what

---

[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] 15 U.S.C. § 45.
[118] 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).
[119] In re Microsoft Corp., No C-4069 (2002) (decision and order), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftdecision.pdf.

information participating websites could collect for their children.[120] The agreement requires that Microsoft establish a comprehensive information security program for Passport, and that it must not misrepresent its practices of information collection and usage.[121]

143. The FTC recently found that Sears Holding Management Corporations business practices violated the privacy of its customers.[122] The consent order arose from the company's use of software to collect and disclose users' online activity to third parties, and a misleading privacy policy that did not "adequately [inform consumers as to] the full extent of the information the software tracked."[123] The order requires that the company fully, clearly, and prominently disclose the "types of data the software will monitor, record, or transmit."[124] Further, the company must disclose to consumers whether and how this information will be used by third parties.[125]

144. 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.[126] This was the first enforcement action to "challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[127] Gateway Learning made representations on the site's privacy policy, stating that consumer information would not be sold, rented or loaned to third parties.[128] In violation of these terms, the company began renting personal information provided by consumers, including gender, age and name, to third parties.[129] Gateway then revised its privacy policy to provide for the renting of

---

[120] In re Microsoft Corp., No. C-4069 (2002) (complaint), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf.

[121] In re Microsoft Corp., No. 012 3240 (2002) (agreement containing consent order), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftagree.pdf.

[122] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

[123] 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).

[124] In re Sears Holdings Mgmt. Corp., No. C-4264 (2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

[125] *Id.*

[126] Press Release, FTC, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.

[127] *Id.*

[128] In re Gateway Learning Corp., No. C-4120 (2004) (complaint), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.

[129] *Id.*

consumer information "from time to time," applying the policy retroactively.[130] 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."[131]

145. Furthermore, the FTC has barred deceptive claims about privacy and security policies with respect to personally identifiable, or sensitive, information.[132] 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 from or about consumers."[133] 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.[134] The Commission further ordered the company to establish comprehensive privacy protection measures in relation to its customers' sensitive information.[135]

146. The FTC has undertaken significant enforcement actions against companies that place at risk the personal information of American consumers. In March 2010, the FTC obtained one of its largest settlements on record, $11 million, against LifeLock, Inc.[136] The FTC found that LifeLock had used false claims to promote its identity theft protection services, which it widely advertised by displaying the CEO's Social Security number on the side of a truck. Since 2006, LifeLock's ads claimed that it could prevent identity theft for consumers willing to sign up for its $10-a-month service.[137] FTC's complaint charged that the fraud alerts that LifeLock placed on customers' credit files protected only against certain forms of identity theft and gave them no protection against the misuse of existing accounts, the most common type of identity theft.[138] It also provided no protection against medical identity theft or employment identity theft, in which thieves use personal information to get medical care or apply for jobs.[139] And even for types of identity theft for which fraud alerts

---

[130] *Id.*

[131] In re Gateway Learning Corp., No. C-4120 (2004) (decision and order), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

[132] In re Life is Good, No. C-4218 (2008) (decision and order), *available at* http://www.ftc.gov/os/caselist/0723046/080418do.pdf.

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] FTC, *LifeLock Will Pay $12 Million to Settle Charges by the FTC,* March 9, 2010, http://www.ftc.gov/opa/2010/03/lifelock.shtm.

[137] *Id.*

[138] *Id.*

[139] *Id.*

are most effective, they did not provide absolute protection. In addition to its deceptive identity theft protection claims, LifeLock allegedly made claims about its own data security that were not true.[140] According to the FTC, LifeLock routinely collected sensitive information from its customers, including their social security numbers and credit card numbers.[141] The FTC charged that LifeLock's data was not encrypted, and sensitive consumer information was not shared only on a "need to know" basis.[142] In fact, the agency charged, the company's data system was vulnerable and could have been exploited by those seeking access to customer information.[143]

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

147. Just last year, Facebook stated 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."[144]

148. Facebook's changes to users' privacy settings and associated policies in fact designate users' names, profile photos, lists of friends, pages, gender, geographic regions, and networks to which they belong as "publically available information."[145] Those categories of user data are no longer subject to users' privacy settings.

149. Facebook has essentially forced many Facebook users to reveal personal profile information that they did not intend to make public. This information includes music, film and literary preferences; geographic information; educational information; and employment information.

150. Facebook's disclosure of user information through the recent changes in business practices violate user expectations and are contrary to representations that Facebook has repeatedly made about privacy protection and users control of personal information.

---

[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] 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.
[145] Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Dec. 13, 2009).

151. Facebook's opt-out for "instant personalization" is difficult for users to find, unduly complicated, and deceptive. There is no way for users to opt-out with one click. Instead, users must go to each separate application in what will be a universe of ever-expanding applications, and opt-out from each individually. Not only does such an approach fail to scale, it is clearly intended to discourage users from exercising privacy controls.

152. 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.

153. Absent injunctive relief by the Commission, Facebook is likely to continue its unfair and deceptive business practices and harm the public interest, as evidence by the company's repeated changes to its privacy policy and aggressive efforts to make more user data "publicly available."

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

V. Prayer for Investigation and Relief

155. Petitioners request that the Commission investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users. Specifically, Petitioners ask the Commission to:

> Compel Facebook to restore its previous privacy settings allowing users to choose whether to link and publicly disclose personal information, including name, current city, friends, employment information, educational information, and music, film, television, and literature preferences;
>
> Compel Facebook to restore its previous requirement that developers retain user information for no more than 24 hours;
>
> 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.

156. Petitioners reserve 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
Ginger McCall, EPIC Staff Counsel
Veronica Louie, EPIC Clerk

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

The Bill of Rights Defense Committee
The Center for Digital Democracy
The Center for Financial Privacy and
Human Rights
The Center for Media and Democracy
Consumer Federation of America
Consumer Task Force for Automotive Issues
Consumer Watchdog
Foolproof Initiative
Patient Privacy Rights
Privacy Activism
Privacy Journal
Privacy Rights Clearinghouse
The United States Bill of Rights Foundation
U.S. PIRG

May 5, 2010