

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION

In the Matter of Myspace, LLC

“FTC File No. 102 3058”

June 8, 2012

---

By notice published on May 14, 2012, the Federal Trade Commission (“FTC”) has proposed a consent agreement with Facebook that would settle “alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition.”<sup>1</sup> Pursuant to this notice, the Electronic Privacy Information Center (“EPIC”) submits these comments and recommendations to ensure that the final order adequately protects the privacy of Myspace users.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.<sup>2</sup> EPIC’s 2010 complaint concerning Google Buzz provided the basis for the Commission’s investigation and October 24, 2011 subsequent settlement concerning

---

<sup>1</sup> Myspace, LLC; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 28388 (proposed May 14, 2012), <http://ftc.gov/os/fedreg/2012/05/120514myspace.pdf> [hereinafter “Myspace Proposed Consent Order”].

<sup>2</sup> See, e.g., Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), [http://epic.org/privacy/internet/ftc/ftc\\_letter.html](http://epic.org/privacy/internet/ftc/ftc_letter.html); DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), [http://epic.org/privacy/internet/ftc/DCLK\\_complaint.pdf](http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf); Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), [http://epic.org/privacy/consumer/MS\\_complaint.pdf](http://epic.org/privacy/consumer/MS_complaint.pdf); Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), <http://epic.org/privacy/choicepoint/fcraltr12.16.04.html>.

the social networking service.<sup>3</sup> In that case, the Commission found that Google “used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz].”<sup>4</sup> The Commission’s settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of privacy and civil liberties organization in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.<sup>5</sup>

Regarding Myspace, EPIC supports the findings in the FTC Complaint and supports the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the Order is insufficient to protect the privacy of Myspace users. EPIC urges the Commission to (1) make the Myspace Order at least as protective as the Commission’s Facebook consent order, and (2) require the Myspace to conform to the substantive protections of the President’s Consumer Privacy Bill of Rights (“CPBR”).<sup>6</sup>

## **I. The FTC’s Myspace Complaint**

The Commission’s Complaint charged that Myspace had engaged in deceptive practices by making personally identifiable information (“PII”) available to advertisers while representing to users that such information would not be disclosed without their permission. According to the Commission investigation, Myspace assigns each of its users a unique identifier called a “Friend

---

<sup>3</sup> Press Release, Federal Trade Comm’n, FTC Charges Deceptive Privacy Practices in Google’s Rollout of Its Buzz Social Network (Mar. 30, 2011), <http://ftc.gov/opa/2011/03/google.shtm> (“Google’s data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.”).

<sup>4</sup> *Id.*

<sup>5</sup> Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), <https://epic.org/privacy/infacebook/EPIC-FacebookComplaint.pdf> [hereinafter EPIC 2009 Facebook Complaint]; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief) [hereinafter EPIC 2009 Facebook Supplement]; Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , [https://epic.org/privacy/facebook/EPIC\\_FTC\\_FB\\_Complaint.pdf](https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf) [hereinafter EPIC 2010 Facebook Complaint].

<sup>6</sup> White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> [hereinafter White House, CPBR].

ID.”<sup>7</sup> The Friend ID allows access to a user’s basic profile information.<sup>8</sup> Myspace allowed third-party advertisers to access personal information by (1) using the Friend ID to view a user’s basic profile information, and (2) linking the Friend ID (and this basic profile information), with the information on the advertiser’s tracking cookie.<sup>9</sup> Many advertising networks that show advertisements on Myspace and other sites across the web place tracking cookies on users’ browsers that contain unique identifiers and a partial history of their web-browsing activity. Myspace allowed advertisers to access this personal information despite promising its users that “MySpace will notify you of your options regarding our use of your PII” and “Myspace will not share your PII with third parties unless you have given Myspace permission to do so.”<sup>10</sup>

These practices resulted in four counts in violation of the FTC Act. Count I alleged that Myspace “provided the Friend ID of the viewing user to third-party advertisers who are not affiliated with Myspace” despite representing that it would not share PII with third parties without first giving notice to and receiving permission from that user.<sup>11</sup> Count II alleged that Myspace “customized ads in numerous instances [in a way that] transmitted the Friend ID of the viewing user to third-party advertisers” despite representing that “the means through which it customize[d] ads d[id] not allow advertisers to access PII or individually identify users.”<sup>12</sup> Count III alleged that Myspace allowed advertisers to “link web browsing activity with the personal information available in a user’s Myspace profile” despite representing that “users’ web browsing activity shared with advertisers [was] anonymized.”<sup>13</sup> Finally, Count IV alleged that Myspace had violated the Notice and Choice requirements of the Department of Commerce’s

---

<sup>7</sup> Myspace, LLC, FTC File No. 102 3058 (2012) (Complaint) 2, available at <http://ftc.gov/os/caselist/1023058/120508myspacecmpt.pdf>.

<sup>8</sup> *Id.* at 3.

<sup>9</sup> *Id.* at 4.

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at 5.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* at 6.

US-EU Safe Harbor privacy principles, despite claiming to adhere to the Safe Harbor Framework.<sup>14</sup>

## II. The FTC's Myspace Consent Order

Part I of the Order bars Myspace from misrepresenting “in any manner, expressly or by implication . . . the extent to which it maintains the privacy or security of covered information.”<sup>15</sup> The prohibition on misrepresentation includes, but is not limited to, the collection or disclosure of covered information, the extent to which a consumer can control the privacy of any covered information, and the extent to which Myspace has made covered information available to third parties.<sup>16</sup> The prohibition on misrepresentation also includes the extent to which Myspace complies with the U.S.-EU Safe Harbor Framework.<sup>17</sup>

Part II of the Order requires Myspace to implement a “comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.”<sup>18</sup> The program must be “documented in writing” and appropriate to Myspace’s size and complexity, nature and scope of activities, and the sensitivity of the covered information.<sup>19</sup>

The program must identify “reasonably foreseeable, material risks” to privacy and describe the controls and procedures that Myspace will take to address those risks.<sup>20</sup> Myspace must also use reasonable steps to ensure that service providers are capable of protecting the

---

<sup>14</sup> *Id.* at 6-7.

<sup>15</sup> Myspace, LLC, FTC File No. 102 3058 (2012) (Agreement Containing Consent Order) 2, *available at* <http://ftc.gov/os/caselist/1023058/120508myspaceorder.pdf>.

<sup>16</sup> *Id.* at 3.

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

privacy of covered information that they receive from Myspace.<sup>21</sup> Finally, Myspace must evaluate and adjust the privacy program in light of changes in business arrangements or the results of regular testing required by the program itself.<sup>22</sup>

Part III requires Myspace to obtain biennial assessments from a “qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession.”<sup>23</sup> This person must have at least three years of experience in the field of privacy and data protection, and must be approved by the FTC.<sup>24</sup> The first report is due 180 days after the order takes effect; subsequent assessments are due every two years for the next 20 years.<sup>25</sup> The assessments must explain the privacy controls implemented and how they are appropriate to meet the requirements imposed by the Order.<sup>26</sup>

Parts IV through VIII contain various procedural details and requirements, such as the requirement that Myspace deliver a copy of the Order to officers and directors who have supervisory responsibilities relating to the subject matter of the Order, and the provision that terminates the Order twenty years from the date of issuance, or twenty years from the most recent FTC complaint alleging a violation of the order, whichever comes later.<sup>27</sup>

### **III. EPIC’s Assessment and Recommendations**

Overall, EPIC supports the findings in the FTC Complaint and supports, in part, the directives contained in the Consent Order. The Order makes clear that companies should not engage in unfair and deceptive trade practices, particularly in the collection and use of personal data. However, the proposed Order fails to implement many of requirements of the

---

<sup>21</sup> *Id.* at 4.

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> *Id.* at 5, 6.

Commission’s consent order with Facebook, and focuses on prohibiting Myspace from deception regarding its practices rather than establishing privacy safeguards on the user data itself. To better protect the interests of Myspace users and fulfill the Commission’s statutory obligation to act in the public interest,<sup>28</sup> EPIC urges the Commission to strengthen the Order in the manner detailed below.

First, the Order should be at least as protective as the Commission’s previous order with Facebook. The Facebook order required Facebook to obtain affirmative, opt-in consent before materially exceeding the privacy settings of users.<sup>29</sup> Facebook was required to “clearly and prominently” disclose to the user (1) the type of information that will be disclosed, (2) the identity of the third parties, and (3) that such disclosure exceeds the restrictions imposed by the privacy settings in effect.<sup>30</sup> Facebook was also required to obtain the user’s “affirmative express consent.”<sup>31</sup> The Facebook order also defines the term “third party.”<sup>32</sup>

None of these protections against disclosure to third parties are present in the Myspace Order. Because both cases relate to social networking services and implicate the collection and use of personally identifiable information, the Commission should require similar protections in each. Furthermore, given that the basis for the Commission’s original complaint was the

---

<sup>28</sup> The Federal Trade Commission Act directs that enforcement actions be commenced against unfair and deceptive trade practices “if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public.” 15 U.S.C. § 45(b) (2010); *see also* *FTC v. Cinderella Career & Finishing Schools, Inc.*, 404 F.2d 1308, 1314 (D.C. Cir. 1968) (noting that “the Commission is charged by the broad delegation of power to it to eliminate unfair or deceptive business practices in the public interest . . . .”); *Scientific Mfg. Co. v. Fed. Trade Comm’n*, 124 F.2d 640, 643-44 (3d Cir. 1941) (“The change effected by the amendment lay in the fact that the Commission could thenceforth prevent unfair or deceptive acts or practices in commerce which injuriously affected the public interest alone, while under the original Act the Commission’s power to safeguard the public against unfair trade practices depended upon whether the objectionable acts or practices affected competition.”); *Rothschild v. Federal Trade Comm’n*, 200 F.2d 39, 42 (7th Cir. 1952) (“One of the purposes of the Act has been the protection of the public, and public interest may exist even though the practice deemed to be unfair does not violate any private right.”).

<sup>29</sup> Facebook, Inc., FTC File No. 092 3184 (2011) (Agreement Containing Consent Order), *available at* <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

unconsented disclosure of personal information, these omissions are particularly noticeable. Although Myspace’s privacy policy prohibits the company from “shar[ing] your PII with third parties unless you have given Myspace permission to do so,” there is nothing in the Order that would prevent Myspace from changing this provision. Indeed, there is little in the Order that would prevent Myspace from changing any of its privacy practices in the future, so long as those practices were accurately described in a revised policy

The Facebook order also contains a data deletion requirement.<sup>33</sup> Facebook must ensure that a user’s information cannot be accessed by a third party from Facebook’s servers “after a reasonable period of time, not to exceed thirty (30) days” from the time the user has deleted the account.<sup>34</sup> The Commission should place a similar provision in the Myspace Order.

Second, the Commission should require Myspace to implement the Fair Information Practices outlined in the Consumer Privacy Bill of Rights. The President has recently set out a comprehensive framework for privacy protection – the Consumer Privacy Bill of Rights (CPBR) – that provides substantive privacy protections for users.<sup>35</sup> The CPBR enumerates seven principles: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.<sup>36</sup> These principles are central to the right of privacy, and appear in numerous frameworks, such as the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines<sup>37</sup> and the Privacy Act of 1974.<sup>38</sup>

---

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> See White House, CPBR.

<sup>36</sup> *Id.*

<sup>37</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html).

<sup>38</sup> Privacy Act of 1974, 5 USC § 552a.

Several of these principles are also highlighted in the Commission's recent report, such as privacy by design, choice, and transparency.<sup>39</sup>

These principles would impose certain requirements on the collection and use of personal information in the social networking context. For example, Individual Control and Respect for Context would require that users consent to new uses or disclosures of their information, such as disclosure to a third-party advertiser. And Transparency and Access and Control would require that users be able to access all of the data that Myspace keeps about them. The right to access increases awareness by giving users the ability to see the full extent of the data collected by a company. The right to access increases users' control by placing the locus of ownership closer to the user, who gains the ability to inspect data and take steps to correct errors. Facebook already provides users with partial access to data that Facebook keeps about them.<sup>40</sup> EPIC has previously called on Facebook to expand user access, thus allowing users to "Know What They Know."<sup>41</sup> Transparency also would require the Commission to make Myspace's privacy audits publicly available to the greatest extent possible.

Finally, the Commission should also make Myspace's privacy audits publicly available to the greatest extent possible. Although companies may exempt trade secrets or confidential commercial information, Part III indicates that portions of the assessments should be able to be completed without revealing any confidential information, such as "the specific privacy controls that [Myspace] has implemented," an explanation of how such controls are "appropriate" to the

---

<sup>39</sup> Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (2012), <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

<sup>40</sup> Miranda Miller, *Your Facebook Data File: Everything You Never Wanted Anyone to Know*, SEARCH ENGINE WATCH (Oct. 3, 2011), <http://searchenginewatch.com/article/2114059/Your-Facebook-Data-File-Everything-You-Never-Wanted-Anyone-to-Know>; Tom Loftus, *Europeans to Facebook: Where's My Data?*, WALL STREET JOURNAL TECHNOLOGY NEWS AND INSIGHTS (Sept. 29, 2011 5:58PM), <http://blogs.wsj.com/digits/2011/09/29/europeans-to-facebook-wheres-my-data/?KEYWORDS=max+schrems>.

<sup>41</sup> EPIC, #KWTK, <https://epic.org/privacy/kwtk/default.html>.



nature of Myspace's activities, and a certification that such controls are sufficiently effective to protect privacy and comply with the terms of the order.<sup>42</sup>

In the past, the Commission has stated that similar privacy assessments by other companies would be available to the public, subject to applicable laws. After finalizing a consent order with Google that required similar independent assessments, the Commission wrote to EPIC and stated that “[t]o the extent permissible under law, the public may have access to the submissions required pursuant to the order.”<sup>43</sup> Furthermore, the experience of the international community provides evidence of the feasibility of such transparency. In 2009, Canadian Privacy Commissioner conducted an investigation of Facebook's privacy policies and released a 113-page report that described in detail the findings of the investigation and the office's recommendations.<sup>44</sup> More recently, the Irish Data Protection Commissioner's investigation into Facebook, cited above, produced a 150-page report and 77 pages of “technical analysis” that were made publicly available.<sup>45</sup>

## **VI. Conclusion**

EPIC supports the findings made by the Federal Trade Commission in the investigation of Myspace. However, users' privacy would be better protected by making the Order at least as protective as the Facebook order, and by requiring the substantive protections of the CPBR.

EPIC urges the Commission to adopt the changes to the proposed Order set out above.

---

<sup>42</sup> Myspace LLC., FTC File No. 102 3058 (2012) (Agreement Containing Consent Order) 4, *available at* <http://ftc.gov/os/caselist/1023058/120508myspaceorder.pdf>.

<sup>43</sup> Letter from Federal Trade Comm'n, Office of Secretary, to EPIC (Oct. 13, 2011), <http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf>.

<sup>44</sup> OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. (2009), [http://www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.cfm#complaint](http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm#complaint).

<sup>45</sup> *See* Data Protection Comm'r, Report of Audit (2011), <http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf>.

Respectfully Submitted,

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