COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

Privacy Roundtables - Comment, Project No. P095416

January 26, 2010

Introduction

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.[1] 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."[2] As a result of the EPIC complaint, the FTC fined Choicepoint $15 million.[3]

EPIC initiated the complaint to the FTC regarding Microsoft Passport.[4] The Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[5] EPIC also filed a complaint with the FTC regarding the marketing of amateur spyware,[6] 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

---

[1] *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.

[2] *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.

[3] 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.

[4] *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.

[5] *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.

[6] *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.

spy on other individuals.[7] More recently, EPIC asked the FTC to investigate the "parental control" software firm Echometrix.[8] Thus far, the FTC has failed to announce any action in this matter, but once the Department of Defense became aware of the privacy and security risks to military families, it removed Echometrix's software from the Army and Air Force Exchange Service, the online shopping portal for military families.[9]

EPIC's Executive Director Marc Rotenberg testified at the first FTC Privacy Roundtable held in Washington, D.C. on December 7, 2009. EPIC Associate Director Lillie Coney will participate in the second roundtable in San Francisco, CA. This comment discusses challenges that innovations in the digital environment pose for consumer privacy, focusing on cloud computing and third-party application developers in a social networking context.

Cloud Computing

1. Privacy Implications of Cloud Computing

Cloud computing continues to have important privacy implications for consumers today. According to a Pew Internet & American life Project report from 2008, 69% of Americans are making use of "cloud computing," allowing their data to reside in online servers accessible via the internet.[10] In an October 2009 study conducted by Penn, Schoen & Berland Associates, 87% of respondents were still not familiar with how cloud computing worked, yet 85% responded they would be concerned about the security of information stored in a "cloud," or online server.[11]

In February 2009, the World Privacy Forum published a report on the risks to privacy and confidentiality from cloud computing.[12] Robert Gellman, who prepared the report, found "a user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider."[13] Further, "for some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider."[14]

---

[7] 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.
[8] *In the Matter of Echometrix, Inc.*, Request for Investigation and for Other Relief, before the Federal Trade Commission (Sep. 25, 2009), *available at* http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.
[9] EPIC, *Excerpts from Echometrix Documents*, http://epic.org/privacy/echometrix/Excerpts_from_echometrix_docs_12-1-09.pdf.
[10] John Horrigan, Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services* (September 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.
[11] Penn, Schoen & Berland Associates, *Online Exposure, Offline Uncertainty: Privacy and Security in a Virtual World* (October 2009).
[12] Robert Gellman, World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (February 2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.
[13] *Id.* at 6.
[14] *Id.*

One of the privacy implications of cloud computing noted in the WPF report is that the transfer of otherwise personal information to cloud providers creates new opportunities for information to be accessed by the government without notice to users.[15] For users, "the loss of notice of a government demand for data is a significant reduction in rights."[16] Another concern is the security of user information: "security requirements for information may also create problems because of the inability of the user to assess the provider's security, to audit security for compliance, or to determine whether the level of security meets statutory or regulatory security requirements."[17]

2. EPIC's FTC Complaint regarding Cloud Computing

In March 2009, the Electronic Privacy Information Center (EPIC) submitted to the Federal Trade Commission (FTC) a complaint,[18] pursuant to Section 5 of the FTC Act, detailing the privacy and security risks of Google's cloud computing-based services. A subsequent letter by thirty-eight computer researchers and academicians to Google CEO Eric Schmidt raised similar concerns.[19]

EPIC's FTC complaint came after a Google security breach, in which "Google disclosed user-generated documents saved on its Google Docs Cloud Computing Service to users of the service who lacked permission to view the files."[20] The complaint cited three other, similar breaches involving Google cloud computing services. EPIC alleged that Google made misrepresentations concerning the security of users' information, and that Google's inadequate security is an unfair business practice and a deceptive trade practice. EPIC concluded,

> The Google Docs Data Breach highlights the hazards of Google's inadequate security practices, as well as the risks of Cloud Computing Services generally. The recent growth of Cloud Computing Services signals an unprecedented shift of personal information from computers controlled by individuals to networks administered by corporations. . . . As a result of the popularity of Cloud Computing Services, data breaches on these services pose a heightened risk of identity theft.[21]

Since EPIC filed the FTC complaint, cloud computing has become increasingly common. The topic has become an international concern for privacy officials. In November 2009, the European Network and Information Security Agency released a report on cloud computing,

---

[15] *Id.* at 11.
[16] *Id.*
[17] *Id.* at 22.
[18] *See generally* EPIC FTC Complaint, *In re Google* (Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[19] Jacob Appelbaum, et al., Letter to Google CEO Eric Schmidt re: Ensuring Adequate Security in Google's Cloud based Services (June 16, 2009), *available at* http://files.cloudprivacy.net/google-letter-final.pdf.
[20] *See supra* note 18, at 8.
[21] *Id.* at 14.

recommending that European officials determine the application of data protection laws to cloud computing services.[22] The report also considers whether personal data may be transferred to countries lacking adequate privacy protection, whether customers should be notified of data breaches, and rules concerning law enforcement access to private data.[23]

In the United States, the federal government has become interested in using cloud computing services. In September 2009, Chief Information Officer Vivek Kundra announced the launch of "Apps.gov," a website where federal agencies can obtain cloud-based IT services.[24] The initiative is aimed at "lowering the cost of government operations while driving innovation."[25] In a speech about the cloud computing initiative, Kundra stated, "Why should the government pay for and build infrastructure that is available for free? In these tough economic times, the federal government must buy smarter."[26] Currently, the administration's main goal is to increase the size and scale of cloud computing,[27] but key concerns, such as security and privacy of citizens' information, have received little attention.

The FTC indicated in a recent comment to the FCC that it was pursuing an investigation on Cloud Computing services but the scope and purpose of the investigation remains unclear. Meanwhile, consumers are increasingly subject to new business practices and shifting privacy policies that leave essential questions about the security and privacy of personal information stored on remote servers unanswered.

3. Recommendations to the FTC regarding Cloud Computing

The FTC has stated that consumer privacy and data security are an "area of priority and emphasis for the Chairman and the entire Commission."[28] Even Microsoft Corporation, which is making a transition towards cloud computing, realizes the importance of privacy and security with respect to cloud computing initiatives. In a call for regulation of cloud computing services, Microsoft General Counsel Brad Smith stated, "Before the promise of cloud computing can fully be realized, we must address users' concerns that moving data to the cloud might render it less secure and less private."[29]

Laws and regulations regarding cloud computing are unclear. As the protectors of American consumers, the FTC should thoroughly investigate the privacy implications of cloud

---

[22] ENISA, *Cloud Computing: Benefits, Risks, and Recommendations for Information Security* (November 2009), *available at* http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
[23] *See id.*
[24] Vivek Kundra, White House Blog, *In the Cloud* (Sep. 15, 2009), *available at* http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud/.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Eileen Harrington, FTC Bureau of Consumer Protection, Letter to: Marc Rotenberg re: EPIC Cloud Computing Complaint (Mar. 18, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.
[29] Celia Kang, *Microsoft Calls for Regulation over Cloud Computing*, Wash. Post Tech Blog, *available at* http://voices.washingtonpost.com/posttech/2010/01/microsoft_calls_for_regulation.html.

computing and hold accountable purveyors of cloud computing services when service providers make repeated, unequivocal promises to consumers regarding information security. Responding to EPIC's complaint on cloud computing and urging the Federal Communications Commission to consider the privacy implications of cloud computing in formulating the National Broadband Plan, due to Congress next month, is a good start to the goal of protecting consumers and consumer information in a cloud computing context.

The FTC should also focus on researching effective privacy-enhancing techniques. Personally identifiable information should not be collected unless absolutely necessary. Further, the FTC should explore techniques of anonymization that provide for actual de-identification of data that cannot be combined with other information for re-identification. Because not all de-identification techniques adequately anonymize data, it is important that the process employed is robust, scalable, transparent, and shown to provably prevent the identification of consumer information.[30]

Third-party applications and Social Networking

1. Privacy Threats of Social Networking and Third-Party Applications

Increased sharing of information in a social networking context continues to be a serious privacy concern for users. While social networking sites foster communication and sharing between members, users should have meaningful control over their information. The notice and choice approach, which has never been an effective means for online privacy, is a particularly bad policy approach when companies are free to revise their privacy settings or to disown the obligation to safeguard privacy all together.[31]

Social networking poses several privacy threats. Many social networking sites, including Facebook, make use of third-party applications.[32] In downloading applications, users are subject to inconsistent privacy policies.[33] Third-party application developers have their own privacy policies and are not subject to the social networking site's privacy policy. Therefore, users who install applications may not have the same privacy protections as they would within the social networking sites.

Furthermore, third-party application developers acquire detailed information about each user and the user's friends. With the case of Facebook, users cannot control this sharing of

[30] *See generally* EPIC, Reidentification Page, http://epic.org/privacy/reidentification/.
[31] *See* Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over*, Read Write Web (Jan. 9, 2010), http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php.
[32] *See, e.g.*, MySpace, Games Apps, http://apps.myspace.com/Modules/AppGallery/Pages/index.aspx?category=7&st=totalinstalls; Facebook, Facebook Platform, http://apps.myspace.com/Modules/AppGallery/Pages/index.aspx?category=7&st=totalinstalls.
[33] *See, e.g.*, Facebook, Statement of Rights and Responsibilities, http://www.facebook.com/terms.php ("When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share.").

information.[34] Certain information is publicly available and thus available to third-party application developers.[35] While users can control whether this information is indexed in a search engine, users cannot control whether this information is given to a third-party application developers.[36] All third-party application developers have access to this information.

As a result, users do not have full control over their information. Even if a user never installs an application, his information is still available to third-party application developers if the user's friend decides to install an application. Users should have the choice whether and what kinds of information to share with third parties.

Unclear privacy policies also pose a major problem for consumers, who may not understand what their consent actually means. Privacy policies have become waivers, rather than policies. Users associate privacy policy with privacy protection. However, this is not the case with many social networking sites. Privacy policies are fluid. There is nothing that stops them from changing. Notice is not enough – users must be given choices with respect to all information. Often, when social networking sites decide to change their privacy policies and settings, they also change users' default preferences. Social networking sites, however, should always keep a user's preference through these transitions.

Further, privacy policies are dense. They are hard to read, more difficult to understand, and are often located at various parts of a webpage. Privacy policies should be written in simple language, or else users become confused, and their consent is no longer meaningful. Many social networking sites do not have a third party review their privacy policy. Facebook is the only one – the social networking site uses TRUSTe's privacy program, and TRUSTe conducts an independent review of Facebook's privacy policy. One problem that still remains with TRUSTe is that the company does not punish its licensees when a licensee compromises consumer trust and privacy.

Another problem with social networking sites is data retention. Once a user's account is deactivated or deleted, information may still reside on Facebook's servers, and if a user decides to reactivate his account, that information will still be available.[37] Users should have the choice whether to deactivate or completely delete their accounts, such that information is permanently removed from all servers. Photos and videos are also often retained on servers, even though they may not be viewable to others.[38] While social networking sites cannot control how a photo is used by other members who have seen or downloaded the photo, there is no reason for Facebook

[34] *See generally* EPIC et al FTC Complaint, *In re Facebook* (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.
[35] *Id.*
[36] *Id.*
[37] Facebook, Privacy Policy, http://www.facebook.com/policy.php ("we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested . . . . Removed and deleted information may persist in backup copies for up to 90 days, but will not be available to others.")
[38] *Id.*

to keep such information on servers. Rather, the information should be deleted from all servers immediately after the user deletes the information from his Facebook account.

2. EPIC's FTC Complaint regarding Facebook's Privacy Practices

In December 2009, EPIC and nine other organizations submitted a complaint to the FTC, detailing the November and December privacy changes by Facebook, which pose threats to users' privacy.[39] The complaint alleged:

> 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.[40]

Facebook's recent privacy changes now require certain information to be "publicly available."[41] Therefore, users can no longer control who sees their user name, profile photos, list of friends, pages they are fans of, gender, geographic regions, and networks to which they belong.[42] While users may opt out of the Facebook Platform, their information will still be shared if a Facebook friend uses a third-party application.[43] Prior to the changes, only a user's name and network were automatically publicly available.

Furthermore, Facebook's representations concerning information shared with third-party application developers are misleading. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can see.[44] The primary "privacy setting" that Facebook demonstrates to third-party developers governs what other users can see from the application's output, rather than what data may be accessed by the application.[45]

Subsequent to petitioners' filing of the complaint, Facebook made several representations. Spokesperson Barry Schnitt asserted, "We discussed the privacy program with many regulators, including the F.T.C., prior to launch and expect to continue to work with them

---

[39] *See supra* note 18.
[40] *Id.* at 25.
[41] *Id.* at 8.
[42] *Id.*
[43] *Id.*
[44] Facebook, *About Platform*, http://developers.facebook.com/about_platform.php.
[45] Facebook Developer Wiki, *Anatomy of a Facebook App*, http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App#Privacy_Settings (last visited Dec. 16, 2009).

in the future."[46] Another spokesperson, Andrew Noyes, also stated that the company spoke with the FTC before the changes. He explained, "We've had productive discussions with dozens of organizations around the world about the recent changes . . . ."[47] In response to these public statements, FTC chairman Jon Leibowitz stated,

> We aren't generally in the business of giving general advisory opinion in advance. I certainly don't think anyone would suggest that we would pre-clear their new privacy policy. It may be good. It may be better or it may not be better. But we aren't the film industry; we don't greenlight like the film industry does.[48]

EPIC received a letter from FTC Bureau of Consumer Protection Director, stating that EPIC's complaint raises issues "of particular interest" to the federal agency, and stressed the importance of providing "transparency about how this data is being handled, maintained, shared, and protected . . . ."[49] EPIC subsequently submitted a supplemental complaint to the FTC, providing further evidence of Facebook's "unfair and deceptive trade practices."[50] Still, the FTC could not confirm or deny that an investigation into EPIC's complaint is ongoing.

---

[46] *See, e.g.*, Brad Stone, *Privacy Group Files Complaint on Facebook Changes*, N.Y. Times (Dec. 17, 2009), *available at* http://bits.blogs.nytimes.com/2009/12/17/privacy-group-files-complaint-on-facebook-privacy-changes/; Alexei Oreskovic, *Facebook Privacy Backlash in FTC's Hands*, Reuters (Dec. 18, 2009), *available at* http://blogs.reuters.com/mediafile/2009/12/18/facebook-privacy-backlash-in-ftcs-hands/; Jessica A. Vascellaro, *Groups File Facebook Complaint*, Wall Street Journal at B7 (Dec. 18, 2009), *available at* http://online.wsj.com/article/SB10001424052748704238104574602262735234366.html; Jacqui Cheng, *FTC Complaint Says Facebook's Privacy Changes are Deceptive*, Ars Technica (Dec. 21, 2009), *available at* http://arstechnica.com/tech-policy/news/2009/12/ftc-complaint-says-facebooks-privacy-changes-are-deceptive.ars; Robert McMillan, *Privacy Groups Bring Facebook Complaints to FTC*, ComputerWorld (Dec. 17, 2009), *available at* http://news.idg.no/cw/art.cfm?id=9E5BB9A6-1A64-67EA-E40759B3AFCD4AC7.

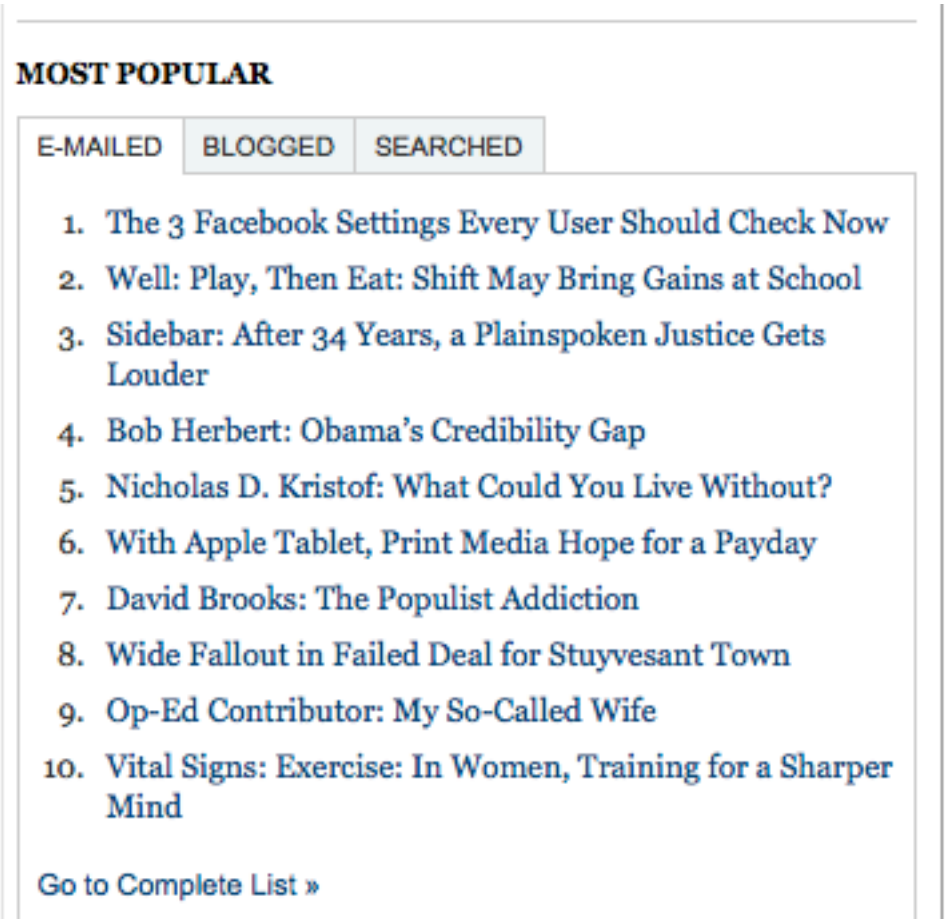
[47] *See, e.g.*, Barbara Ortutay, *Privacy Watchdog Files Complaint against Facebook*, Washington Post (Dec. 17, 2009), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/17/AR2009121702842.html; Peter Kafka, *Next Step in Facebook Privacy Blowback: The FTC Complaint. The Real Question: Will Advertisers Care?*, All Things Digital (Dec. 17, 2009); *available at* http://mediamemo.allthingsd.com/20091217/next-step-in-the-facebook-privacy-blowback-the-ftc-complaint-will-advertisers-care/; John Letzing, *Privacy Groups file FTC Complaint against Facebook*, MarketWatch (Dec. 17, 2009), *available at* http://www.marketwatch.com/story/privacy-groups-file-ftc-complaint-against-facebook-2009-12-17; Ryan Singel, *Facebook Privacy Changes Break the Law, Privacy Groups Tell FTC*, Wired (Dec. 17, 2009), *available at* http://www.wired.com/epicenter/2009/12/facebook-ftc-complaint/; Katherine Noyes, *Privacy Groups Take Facebook Quarrel to the Feds*, Tech News World (Dec. 18, 2009), *available at* http://www.technewsworld.com/story/68939.html; JC Raphael, *Facebook Ignites War of Worlds*, PC World (Dec. 17, 2009), *available at* http://www.pcworld.com/article/185033/facebook_privacy_complaint_ignites_war_of_words.html.

[48] Cecilia Kang, *FTC to Facebook: We aren't in the movie business, we don't greenlight privacy policies*, Wash. Post (Jan. 4, 2010), *available at* http://voices.washingtonpost.com/posttech/2010/01/jon_leibowitz_chairman_of_the.html.

[49] David Vladeck, FTC Bureau of Consumer Protection, Letter to Marc Rotenberg re: EPIC, et al. Facebook Complaint (Jan. 14 2010), *available at* http://epic.org/privacy/inrefacebook/Facebook_Vladeck_Letter.pdf.

[50] EPIC, et al. FTC Supplemental Complaint, *In re Facebook* (Jan. 14, 2010), *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf.

And since these recent developments, an article has highlighted the ongoing public concerns about Facebook and privacy. "The 3 Facebook Settings Every User Should Check Now,"[51] has remained the most popular article on the New York Times web site for several days.



MOST POPULAR

E-MAILED | BLOGGED | SEARCHED

1. The 3 Facebook Settings Every User Should Check Now
2. Well: Play, Then Eat: Shift May Bring Gains at School
3. Sidebar: After 34 Years, a Plainspoken Justice Gets Louder
4. Bob Herbert: Obama's Credibility Gap
5. Nicholas D. Kristof: What Could You Live Without?
6. With Apple Tablet, Print Media Hope for a Payday
7. David Brooks: The Populist Addiction
8. Wide Fallout in Failed Deal for Stuyvesant Town
9. Op-Ed Contributor: My So-Called Wife
10. Vital Signs: Exercise: In Women, Training for a Sharper Mind

Go to Complete List »

But as one commentator has noted, every single recommendation in the article is about how to make the user profile more private not less private.[52] In FTC terms, consumers are trying to restore the privacy settings they had prior to the recent changes made by Facebook. And this is among the top concerns today of American consumers.

3. Success of Efforts by Privacy Officials Abroad

Privacy and consumer protection officials in other countries have been active in responding to privacy threats posed by online companies, and have been met with a strong response. The Canadian Privacy Commission has pursued several investigations

[51] Sarah Perez, *The 3 Facebook Settings Every User Should Check Now*, N.Y. Times (Jan. 20, 2010), *available at* http://www.nytimes.com/external/readwriteweb/2010/01/20/20readwriteweb-the-3-facebook-settings-every-user-should-c-29287.html?em.

[52] Daniel Sieberg, "The Privacy Factor – tech Talk – CBS News," (Jan. 25, 2010), available at http://www.cbsnews.com/blogs/2010/01/25/eveningnews/techtalk/entry6141447.shtml

of Facebook's privacy controls and has required the company to increase user privacy. Facebook acknowledged that it made changes in an attempt to improve user privacy on Facebook Platform as "a result of our work with the Office of the Privacy Commissioner of Canada, which has spent more than a year reviewing our privacy policies."[53]

The Canadian Privacy Commissioner took particular interest in Facebook after receiving a complaint filed by Canadian law students. In May 2008, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a 35-page complaint under Canada's Personal Information Protection and Electronic Documents Act against Facebook, alleging 22 separate violations of Canadian privacy law.[54] In mid-July of 2009, after reviewing the CIPPIC complaint, the Canadian Privacy Commission released a report recommending several changes to Facebook's business practices.[55] The Commissioner's Office advised the social networking firm to limit application developers' access to user information, and inform users specifically about the nature and use of shared information.[56] The Office also said that deactivated account information should be deleted, and that the privacy policy be amended to include all intended uses of personal information.[57] Facebook responded to the complaints and worked with the Commissioner to make appropriate changes to improve user privacy in August.[58]

More recently, Canada's Privacy Commissioner has launched an investigation into the information collection and use practices of online social networking sites.[59] This investigation is being conducted as the Parliament prepares to review the Personal Information Protection and Electronic Documents Act.[60] Stoddart plans to examine "issues that we feel pose a serious challenge to the privacy of consumers, now and in the near future," and to foster discussions about "the impact of these technological developments on privacy."[61]

Similarly, Microsoft has responded to complaints by the European Union's Article 29 Working Group, which includes data protection officials from all 27 countries

---

[53] Facebook Blog, *Improving User Privacy on Platform* (Aug. 27, 2009), http://developers.facebook.com/news.php?blog=1&story=292.
[54] Canadian Internet Policy and Public Interest Clinic, PIPEDA Complaint: Facebook (May 30, 2008), *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.
[55] 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.* (July 2008), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.
[56] *Id.*
[57] *Id.*
[58] *See supra* note 49.
[59] The Canadian Press, *Privacy Commissioner looking at how Facebook gets Data*, *available at* http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20100118/facebook_privacy_100118/20100118?hub=SciTech
[60] *Id.*
[61] *Id.*

in the EU.[62] In 2008, the Article 29 Working Group met with Microsoft, Google, and Yahoo, to discuss their data retention practices.[63] Following a determination that records are subject to European privacy law, the Article 29 Working Group asked the search engine companies to eliminate online user data, including IP addresses and search queries, after six months.[64] In order to comply with European privacy law, Microsoft announced that it will delete user search data, including IP addresses, after six months. Microsoft will redesign its new Bing search engine to comply with the request.[65]

Conclusion

Cloud computing and social network services offer substantial new benefits to American consumers but also raise serious privacy and security concerns. The Commission's interest in these topics is appropriate, but its failure to take any meaningful actions, even after the problems have been well documented, reflects a lack of leadership and technical understanding in areas of increasing interest to American consumers.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
Lillie Coney, EPIC Associate Director
Kimberly Nguyen, EPIC Consumer Privacy Counsel

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

[62] Peter Cullen, Chief Privacy Strategist for Microsoft, *Microsoft Advances Search Privacy with Bing*, Microsoft on the Issues (Jan. 18, 2010), http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx.
[63] *Id.*
[64] *Id.*
[65] *Id.*