2010

Online Privacy, Social Networking, and Crime Victimization : Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 111th Cong., July 28, 2010 (Statement by Adjunct Professor Marc Rotenberg, Geo. U. L. Center)

Marc Rotenberg
Georgetown University Law Center, rotenbem@law.georgetown.edu

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on

"Online Privacy, Social Networking, and Crime Victimization"

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives

July 28, 2010
2141 Rayburn House Office Building
Washington, DC

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify today. My name is Marc Rotenberg, and I am the President of the Electronic Privacy Information Center. EPIC was established to focus public attention on emerging privacy and civil liberties issue. I also teach Information Privacy Law at Georgetown University Law Center. I want to thank you for holding this hearing today and also thank Chairman Conyers for his May letter to Facebook.

EPIC has a particular interest in privacy and social networking services. We filed two complaints at the Federal Trade Commission in the last year following decisions by Facebook to change its privacy policies and the privacy settings of its users. We also filed a complaint when Google introduced Buzz, its social network service, because the company essentially opted in all of its Gmail users. We believe it is vitally important to protect the privacy of users of these services, and many users agree.

To be clear, we do not object to social network services—they are enormously valuable—but we do believe that there are serious privacy risks to users resulting from the actions of Facebook that should be pursued. In some instances, we believe that laws were violated and investigations should go forward. In other areas, it may be necessary to enact new laws.

In my testimony today, I will discuss the growing importance of Facebook, the privacy risks to users, and the problems with the current approach to privacy protection. I will also point out that these concerns are widely shared among Facebook users and have been well documented by news reports, user campaigns, and survey data.

Because of the failure of the Federal Trade Commission to take meaningful action to address these problems, I will recommend that the Committee expand statutory privacy safeguards until Title 18 and specifically revise section 2701 of the Electronic Communications Privacy Act ("ECPA") to limit the ability of companies such as Facebook to disclosure user data to third parties, such as application developers and web sites without meaningful opt-in consent.

This change in law will not prevent Facebook from disclosing personal information about its users to third parties. It will simply make the company more transparent and more accountable, and it will give users greater control over the collection and use of their data.

<u>Value of Facebook</u>

Mr. Chairman, there is no question that Facebook is an enormously popular and successful social network service. The numbers are well known—more than

500 million users.[1] If Facebook were a country, it would be larger than the United States, Germany, and Japan combined. Also astonishing is the continued growth of the company, particularly outside of the United States. It is not unreasonable to anticipate that Facebook will, in a few years, have more than a billion members. [2]

Facebook is quickly replacing email as a primary communications tool, particularly when many people are involved. In fact, in preparing for this hearing, I posted a note on my own Facebook page and asked friends to provide ideas for this statement. [3] Many people responded – some I knew well, some hardly at all. But almost all of the suggestions were interesting and helpful. The Public Policy Director of Facebook even joined the discussion. So, there was an opportunity to those who were sending ideas to me to also share their views directly with Facebook.

In similar fashion, all across the social network service, people are organizing, gathering information, sharing ideas, and building communities. There were ways to do this before Facebook, but none as effective or as simple. Much like the telephone service, the use is as broad as the interests and needs of the users.

Of course, recognizing that Facebook is enormously successful does not answer the question of whether Congress has a role to play in protecting the public interest. We are dependent today on many popular technologies, including the telephone and email, where public law and Congressional oversight have helped encourage innovation and competition while safeguarding consumers.

Also, popularity in this context is somewhat double-edged. Although the company has many users, many are also not happy; thousands have joined groups on the service decrying its privacy policies.[4] Privacy continues to be the top concern of users and many polls give Facebook low ratings for customer satisfaction and trust. [5]

---

[1] Mark Zuckerberg, *500 Million Stories*, THE FACEBOOK BLOG, July 21, 2010, http://blog.facebook.com/blog.php?post=409753352130.

[2] *See, e.g.,* Mark Sweeney, *Mark Zuckerberg: Facebook "almost guaranteed" to Reach 1 Billion Users*, THE GUARDIAN (UK), Jun. 23, 2010, *available at* http://www.guardian.co.uk/media/2010/jun/23/mark-zuckerberg-facebook-cannes-lions.

[3] "Facebook| *Marc Rotenberg* I am testifying this week in Congress on Privacy and Facebook (or as the hearing notice says 'Online Privacy, Social Networking, and Crime Victimization.') Your thoughts? Have the changes in FB's privacy settings created serious problems for users? Examples? Thanks for your thoughts on this." *Available at* http://www.facebook.com/marc.rotenberg?v=wall&story_fbid=126089890769520&ref=mf.

[4] *See, e.g.*, Facebook, People Against the new Terms of Service (TOS), administrated by Julius Harper Jr, and Anne Kathrine Yojana Petterøe, http://www.facebook.com/group.php?gid=77069107432; Facebook, Millions Against Facebook's Privacy Policies and Layout Redesigns, administrated by Miki Perrotta and Jessica Fishbein, http://www.facebook.com/group.php?gid=27233634858; Facebook, Bring back News Feed and Wall privacy settings, administrated by Maggie Ds, http://www.facebook.com/group.php?v=wall&gid=204943119385.

[5] *See, e.g.*, ForeSee Results, *Facebook Flops in ACSI E-Business Report*, *available at* http://www.foreseeresults.com/news-events/press-releases/facebook-flops-in-acsi-ebusiness-

Approach to Privacy

Much of the privacy discussion with Facebook typically focuses on what users should or should not post online.[6] But in my opinion, this is a mistake. First of all most users have a good understanding about what not to post. I have never seen anyone put a credit card number or an SSN on his or her wall. People may post embarrassing photos or sharp comments, but this problem is overrated. Most Facebook users put those actions in context and don't give them much concern. And Facebook users quickly learn that they can take down photos and update profiles. Online identity is dynamic and the user experience reflects that.

But there is a problem with Facebook users who try to share information selectively—vacation photos with close friends, organizing information for an upcoming event.[7] Facebook has an elaborate system of privacy setting that the company says allows users to decide how much information to reveal to others.[8] For example: You would generally limit your "wall posts" to friends. You might share photos with certain friends. You would probably only give to third party applications, such as Farmville, the information about you that was actually necessary for the application.

In theory, this is could be a good approach. In practice, Facebook's privacy settings have not worked. They are too confusing, too elaborate, too inconsistent, and too difficult for users to make real decisions. Most Facebook users have no idea

report.shtml (last visited July 23, 2010); PEW INTERNET AND AMERICAN LIFE PROJECT, REPUTATION MANAGEMENT AND SOCIAL MEDIA (May 2010).

[6] *See* Alex Pham, *Internet Security 101: What not to post on Facebook*, Los Angeles Times, May 3, 2010, http://latimesblogs.latimes.com/technology/2010/05/internet-security-what-not-to-post-on-facebook.html; Donna Tapellini, *Consumer Reports Survey: Social Network Uses Post Risky Information,* CONSUMERREPORTS.ORG ELECTRONICS BLOG, May 4, 2010 *http://blogs.consumerreports.org/electronics/2010/05/social-networks-facebook-risks-privacy-risky-behavior-consumer-reports-survey-findings-online-threats-state-of-the-net-report.html*; JR Raphael, *Facebook Privacy: Secrets Unveiled*, PC WORLD, May 16, 2010, http://www.pcworld.com/article/196410/facebook_privacy_secrets_unveiled.html.

[7] *See* Kevin Bankston, *Facebook's New Privacy Improvements Are a Positive Step, But There's Still More Work to Be Done*, EFF DEEPLINKS BLOG, May 26, 2010, http://www.eff.org/deeplinks/2010/05/facebooks-new-privacy-improvements-are-positive.

[8] *See* Facebook, Choose Your Privacy Settings: Basic Directory Information, http://www.facebook.com/settings/?tab=privacy&section=basic&h=043586873d43d155919f99dfb3816a66 (last visited July 27, 2010); Facebook Privacy Guide, http://www.facebook.com/privacy/explanation.php (last visited on July 27, 2010); Robert Strohmeyer, *Facebook's Zuckerberg Answers Critics With New Privacy Controls*, PC WORLD, May 26, 2010, http://www.pcworld.com/article/197261/facebooks_zuckerberg_answers_critics_with_new_privacy_controls.html; Mark Zuckerberg, *Making Control Simple*, THE FACEBOOK BLOG, May 26, 2010, http://blog.facebook.com/blog.php?post=391922327130 (last visited July 27, 2010).

who their information goes to or for what purpose.[9] And Facebook always reserves the right to make personal information "publicly available" regardless of what the user chooses.

Several of the people who commented on my Facebook page described the problem. "Mary Mi" said she could no longer limit the availability of her profile information. Another friend pointed out that it was not easy to control comments on photos. [10] John Nagle wrote that it was basically impossible to turn off certain applications, such as Glifts and pointed out that you often have to go through many screens to set or change privacy settings.

I liked a comment from Ralph T. Castle who said that "the lack of documentation as the single biggest problem in the system." In his words:

> Proper documentation would explain the deeper ramifications of privacy settings (e.g. if you click to say that you "like" something you may receive ads for similar products). Users would then be better empowered a) to make privacy settings and b) to leave FB if they don't like it.

And then there were very extensive comments from Joanne Edwards about the complexity of the settings, the "triple-step privacy" assurances, the news feed settings, the openness of the defaults, and photo-tagging. Ms. Edwards is also an administrator for several important Facebook groups, including "Millions Against Facebook's Privacy Policies and Layout Redesigns," "Protest: Restoring The Age Of Privacy To Facebook' group," and "'Bring Back News Feed and Wall Privacy Settings' group)." The titles of these groups makes clear the concerns of users, and the groups have tens of thousands of members.

But perhaps most remarkably, I have listened to Facebook experts discuss the privacy settings who quickly became confused. I even heard Facebook founder Mark Zuckerberg describe the new changes to his company's privacy settings only to learn, unexpectedly, that some of his college photos were now available to "everyone."[11]

---

[9] *See In the Matter of Facebook, Inc.*, Complaint, Request for Investigation, Injunction, and Other Relief, Before the Federal Trade Commission 15-21 (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.

[10] *See* note 3, *supra*.

[11] Kashmir Hill, *Either Mark Zuckerberg Got a Whole Lot Less Private or Facebook's CEO Doesn't Understand the Company's New Privacy Settings*, TRUE/SLANT, Dec. 10, 2009, http://trueslant.com/KashmirHill/2009/12/10/either-mark-zuckerberg-got-a-whole-lot-less-private-or-facebooks-ceo-doesnt-understand-the-companys-new-privacy-settings/ (last visited July 27, 2010).

I am convinced that not even Facebook understands how its own privacy settings operate. And if Facebook cannot understand the privacy settings, how can the users?[12]

Risks to Users

The problem is serious also because these weaknesses can be exploited by criminals and others. And these data-based crimes can be very difficult to trace back to the source. For example, when a video camera is stolen from the back seat of a car, the owner knows what was taken, approximately when it was taken, and the scope of the damage. But crimes such as identity theft rarely have any of these characteristics. Information can be gathered from several sources. Delay may favor the criminal. The extent of damage is often difficult to determine.[13]

It is only in those cases where investigations are pursued that the link between a user and a sloppy business practice is likely to be established. One of the most well known examples occurred back in 2005 when the data broker Choicepoint publicly disclosed that it had sold personal information on 145,000 consumers to a criminal ring engaged in identity theft.[14] Ironically, the company also sold business verification services, but it did not bother to verify its own sale of consumer data.[15]

That case was of particular interest to EPIC because EPIC had warned the FTC prior to the incident that Choicepoint's lax security practices were placing consumers at risk.[16] The FTC ignored our complaint and one of the largest cases of identity theft occurred. It was only after the harm occurred that the FTC got involved, ultimately issuing its largest fine for a privacy violation in history.[17]

---

[12] Facebook Privacy Policy, http://www.facebook.com/policy.php (last visited on July 27, 2010) ("We cannot ensure that information you share on Facebook will not become publicly available."); *see also* Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, EFF DEEPLINKS BLOG, April 28, 2010, http://www.eff.org/deeplinks/2010/04/facebook-timeline/.

[13] FTC, CONSUMER SENTINEL NETWORK DATABOOK FOR JANUARY-DECEMBER 2009 (FTC February 2010), available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf. *See also* FTC, *FTC Issues Report of 2009 Top Consumer Complaints,* http://www.ftc.gov/opa/2010/02/2009fraud.shtm (identity theft is top complaint of American consumers.)

[14] ChoicePoint, Securities and Exchange Commission Form 8-K, filed March 4, 2005, *available at* http://www.sec.gov/Archives/edgar/data/1040596/000095014405002087/g93611e8vk.htm (last visited July 27, 2010).

[15] *See* EPIC, *Choicepoint*, http://epic.org/privacy/choicepoint/ (last visited July 27, 2010).

[16] EPIC, *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.

[17] Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties*, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited July 27, 2010).

Finding the tie between the cavalier attitude of social network services toward user privacy and the harms users suffered will not be easy. But reports of specific harms resulting from information made available by these services are available, including instances of domestic violence and "outing." For example, anonymous blogger "Harriet Jacobs" revealed that her abusive ex-husband gained access to her current location and workplace because of Google Buzz creating automated lists from email contacts without subscriber consent.[18] Computer science students at MIT looked at a user's Facebook friends and could predict whether the person was gay.[19] In another example, a computer science professor at the University of Texas was able to predict a Facebook user's political affiliation using details from user profiles and friend lists.[20] And researchers at the University of Maryland, College Park found that users' gender could be predicted from user profile information, membership pages, and friend lists.[21]

EPIC Facebook Complaints

Because of the many changes to the Facebook privacy policy, EPIC in collaboration with many other consumer and privacy organizations have asked the FTC to investigate.[22] To be very clear, when the company changes its privacy policies, there is really nothing the user can do. You can't even quit and walk away because Facebook makes it very difficult to permanently delete accounts. [23]

Our complaints to the FTC set out a simple theory – for a company to announce a privacy policy, to sign up a user, and then to change that privacy policy without meaningful consent is an unfair and deceptive trade and practice, or in most

---

[18] Harriet Jacobs, Fugitivus Blog Post: *Fuck You Google* (Feb. 11, 2010), http://gizmodo.com/5470696/fck-you-google.

[19] Carter Jerigan and Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, 14 FIRST MONDAY (2009), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. *See also* Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON.COM, (Sept. 20, 2009), http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/; Steve Lohr, *How Privacy Vanishes Online*, NEW YORK TIMES (March 16, 2010), http://www.nytimes.com/2010/03/17/technology/17privacy.html.

[20] Jack Lindamood, et al, *Inferring private information using social network data*, Proceedings of the 18th International World Wide Web Conference, 1145 (2009), *available at* http://portal.acm.org/citation.cfm?id=1526899.

[21] *See* Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON.COM, (Sept. 20, 2009), http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

[22] *See* EPIC et al FTC Complaint, *In the Matter of Facebook* (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf; EPIC et al FTC Supplemental Materials, *In re Facebook* (January 15, 2010), *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf; EPIC et al FTC Complaint, *In re Facebook* (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

EPIC et al FTC Supplemental Materials, *In re Facebook* (January 15, 2010), 4, *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf.

simple terms, a "bait and switch."[24] That is essentially the problem that Facebook users confronted as well as users of Gmail who find that there email accounts contact information had been made publicly available so that Google could launch a social network service to compete with Facebook.

It is appropriate for the FTC to intervene in these circumstances for the obvious reason that the company is not honoring its part of the bargain but the FTC has been reluctant to do so.[25] That is a problem and has also exposed users to unnecessary risk.

Approaches to Privacy – Regulations, Self-Regulation, Bait and Switch

Congress has taken a variety of approaches to protecting privacy in new online environments. Sometimes, Congress will pass legislation as it did to protect telephone communications many years ago[26] or electronic health records more recently.[27] Congress also passed privacy legislation for email, fax machines, polygraphs, cable television, and many other new services.[28]

Other times Congress may allow industries to regulate themselves under the belief that industry will come up with effective standards that protect consumers. In the privacy world, this self-regulatory approach has always assumed that companies would still remain accountable to their users through the privacy policies that they establish.[29] This means that privacy policies, voluntarily developed by companies, must still be enforceable.[30]

But here is the problem: if the Federal Trade Commission is unwilling or unable to enforce these policies and if individual users are unlikely or unable to bring their claims, then there is no incentive for companies to honor their

---

[24] EPIC et al FTC Complaint, *In the Matter of Facebook*, 1, (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf; EPIC et al FTC Supplemental Materials, *In re Facebook*, 1-2, (January 15, 2010), *available at* http://www.epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf; EPIC et al FTC Complaint, *In re Facebook*, 1, (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[25] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2006).

[26] *See* the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2006); the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.* (2006); *see also* 47 U.S.C. § 605 (2006).

[27] *See* The Health Insurance Portability and Accountability Act of 1996, Privacy Rule, 45 CFR Parts 160 and 164, 67 FED. REG. 53182 (2002).

[28] *See generally* MARC ROTENBERG. THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (EPIC 2005).

[29] In 1999, the Federal Trade Commission published a report setting forth this model. *See* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf.

[30] For a detailed explanation of the need for enforceability, see Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* U.S. DEPARTMENT OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, (1997) *available at* http://ssrn.com/abstract=11472.

commitments. They may get hit with bad press, but that simply turns privacy changes into a public relations problem, which companies have learned to manage in a variety of ways. For example, companies might fund "consumer" organizations so that they are less likely to express criticism over changes in business practices.[31]

This problem is particularly acute with firms such as Facebook, which are becoming—as Mark Zuckerberg has acknowledged—"social utilities," essential services that face no meaningful competition in the marketplace.[32] But

Recommendations

Companies increasingly respond to calls for Congressional action by saying that action by Congress will stifle innovation. But much of the innovation that is being promoted today is not so much about technology, but about marketing. Companies are finding new ways to collect and disclose user data and they do this in ways that make it increasingly difficult for users to understand or control. This is the activity that the companies do not want regulated.

This is evident also in the privacy field where laws have created incentives for better business practices that promote trust and confidence in new services and reduce risks to consumers. For example, many recent privacy laws create obligations for companies offering online services to encrypt communications and stored data.[33] Others make consent meaningful through explicit opt-in requirements.[34]

For Facebook, one of the simplest and most effective ways to give users meaningful control would be to make explicit in statute the need for the company to obtain explicit, opt-in consent for any disclosure that the company makes of user data to third parties. Most notably, section 2701 of the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA)[35] should restrict more forcefully the ability of service providers such as Facebook to share user data with third parties without explicit opt-in consent from users.

It is obvious and commonsense that it is the user who should decide to whom to disclose their data. Facebook can provide many different services that allow, and even encourage users to share data, but the company should not decide for the user

[31] For an in-depth explanation of this problem, see EPIC, Privacy Regulation: A Decade of Disappointment, http://epic.org/reports/decadedisappoint.html.
[32] *See, e.g.*, Joshua Brustein, Facebook is to Power Company as . . . , NY TIMES, July 24, 2010, *available at* http://www.nytimes.com/2010/07/25/weekinreview/25brustein.html.
[33] *See, e.g.*, Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 201 *note* (2010).
[34] *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201 et seq. (2010); HIPAA Administration Simplification, 45 C.F.R. § 164.508-510.
[35] 18 U.S.C. § 2701 et seq. (2010)

what information to share. Whenever that occurs, the user has lost control and has lost privacy.

Conclusion

Mr. Chairman, Facebook is a tremendous service, with the scope of email, the telephone, and even the Internet itself. It is also the source of many of the privacy concerns of users today. The critical problem is not what users post; it is that the Facebook changes the privacy settings too frequently and Facebook makes it too difficult for users to selectively post information. Self-regulation has not worked because the FTC has been reluctant to pursue investigations. So, EPIC recommends changes to ECPA in Title 18 that would give users greater control of their information and reduce risk when they go online.

GENERAL REFERENCES

Dana boyd, “Facebook's paternalistic attitudes aren't empowering,” CNN Tech, June 28, 2010.

Letter from Chairman John Conyers, Jr. to Mark Zuckerberg (May 28, 2010), *available at* http://judiciary.house.gov/hearings/pdf/Conyers-Facebook100528.pdf.

Electronic Privacy Information Center (EPIC), Facebook Privacy, http://epic.org/privacy/facebook/ (last visited Jul. 27, 2010).

EPIC, Social Networking Privacy, http://epic.org/privacy/socialnet/ (last visited Jul. 27, 2010).

EPIC et al. FTC Complaint, *In re Facebook* (Dec. 17, 2009), *available at* http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

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

EPIC et al. FTC Complaint, *In re Facebook II* (May 5, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

EPIC et al. FTC Complaint, *In re Google Buzz* (Feb. 16, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

EPIC et al. FTC Supplemental Complaint, *In re Google Buzz* (Mar. 2, 2010), *available at* http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf

Facebook, People Against the new Terms of Service (TOS), administrated by Julius Harper Jr, and Anne Kathrine Yojana Petterøe, http://www.facebook.com/group.php?gid=77069107432.

Facebook, Bring back News Feed and Wall privacy settings, administrated by Maggie Ds, http://www.facebook.com/group.php?v=wall&gid=204943119385.

Facebook, Millions Against Facebook's Privacy Policies and Layout Redesigns, administrated by Miki Perrotta and Jessica Fishbein, http://www.facebook.com/group.php?gid=27233634858.

DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD (2010).

BEN MEZRICH, THE ACCIDENTAL BILLIONAIRES: THE FOUNDING OF FACEBOOK, A TALE OF SEX, MONEY, GENIUS, AND BETRAYAL (2009).

JOHN PALFREY AND URS, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2009)

Jeffrey Rosen, *The Web Marks the End of Forgetting,* N.Y. TIMES MAGAZINE, July 25, 2010, at 26, *available at* http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

Marc Rotenberg, Op-Ed, *Online friends at what price? The point of social networking is to share your personal information with the world*, SACRAMENTO BEE, July 20, 2008.

Marc Rotenberg, Constructing a Policy Framework for Social Network Services: Distinguishing the Roles and Responsibilities of the Participants, Computers, Privacy, and Data Protection Conference, Brussels, Belgium (Jan. 2009), *available at* http://www.cpdpconferences.org/L-Z/rotenberg.html

Clive Thompson, *Brave New World of Digital Intimacy*, N.Y. TIMES MAGAZINE, Sept. 5, 2008, at 42, *available at* http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html.