

Richard F. Gaspar, Ph.D.

Saving face on Facebook: Educating users' about privacy

In Western culture, individual privacy is a long established basic right. Many laws have been established that safeguard privacy. Categories defining the parameters of privacy have also been created to protect individuals from unreasonable intrusion. However, for social media users, new businesses and modern consumers of news, the established legal definitions may be inadequate. On Jan. 9, 2010, Mark Zuckerberg announced to a live audience, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people" (As cited by Kirkpatrick, 2010). Zuckerberg concluded that online privacy was dead, and so was Facebook's 2005 privacy policy. Facebook's privacy policy changes generated thousands of articles, interviews and debates, as well a formal complaint to the Federal Trade Commission (FTC File No. 092 3184, 2011). In November 2011, Facebook settled the charges that it deceived its users, resulting in an additional overhaul of its privacy policy. In the end, the court challenge established that personal privacy is still important and social media companies should establish policies that protect it. However, many users are unaware of the numerous changes that have taken place to the Facebook's Privacy over the past few years and are still unaware on how to safe guard their personal information and protect privacy.

I. Defining Privacy

In Western culture, individual privacy is a long established basic right. Many laws have been established that safeguard privacy. Categories defining the parameters of privacy have also been created to protect individuals from unreasonable intrusion. Legal cases have also helped define a clearer view of an individual's right to privacy. Justice Dickson provides a definition of privacy applicable to the expectations of most Facebook users: "Privacy may be defined as the right of

the individual to determine when, how, and to what extent he or she will release personal information” (R. v. Duarte, par. 6, 1990). Ethicist Louis Hodges adds, “The moral right to privacy consists of the power to determine who may gain access to information about oneself (1994, par. 1).

Facebook’s 2012 privacy policy states: “We may access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm. Information we receive about you, including financial transaction data related to purchases made with Facebook Credits, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm” (Improve Your Experience, 2012). Facebook also launched the “Facebook Terms and Policies Hub” which holds its 10 policy documents to explain its new “Data Use Policy” (Constantine, 2012). However, Facebook Privacy Policy was not always this complex.

In 2005, Facebook was basically a social network for private exchanges of information with members of choice. Even the Privacy Policy was simple: “No personal information that you submit to ‘The facebook’ will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings” (Opshal, 2010). However, even in 2005, researchers noted problems in Facebook’s Privacy Policy. MIT students Harvey Jones and Jose Soltren examined the wide amount of information users shared on the social networking site. They concluded three main threats existed concerning privacy: “users share too much,

Facebook does not take adequate steps to protect user privacy, and third parties are actively seeing out end-user information using Facebook” (Jones & Soltren, 2005).

In 2006, the policy was adjusted to make the user’s school and location public. A more significant policy change appeared in 2007 when Facebook announced: “Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends)” (Doctorow, 2012). The policy grew in complexity over the next two years, and in 2009, Facebook notified users that much of their personal information was no longer private: “Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook” (Opshal, 2012).

The 2009 Privacy Policy resulted in numerous cases, complaints and lawsuits. The strongest and most powerful complaint came from The Federal Trade Commission (FTC File No. 092 3184, 2011). The case alleged that Facebook:

- Changed its website so certain information that users may have designated as private -- such as their Friends List -- was made public. They didn't warn users that this change was coming, or get their approval in advance.
- Represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data -- data the apps didn't need.
- Told users they could restrict sharing of data to limited audiences -- for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.

- Promised users that it would not share their personal information with advertisers. It did.
- Claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.

Even members of Congress weighed in on the social networks privacy changes. Senators Charles Schumer, Michael Bennett, March Begich and Al Franken sent an “Open Letter” to CEO Mark Zuckerberg to “express our concern regarding recent changes to the Facebook privacy policy and the use of personal data on third party websites.... We hope that Facebook will stand by its goal of creating open and transparent communities by working to ensure that its policies protect the sensitive personal biographical data of its users and provide them with full control over their personal information (Politico, 2010). Government organizations from other nations also began investigating Facebook (Christians, 2012).

CEO Mark Zuckerberg acknowledged the “mistakes” in a blog post on November 19, 2011: “I’m the first to admit that we’ve made a bunch of mistakes. In particular, I think that a small number of high profile mistakes, like Beacon four years ago and poor execution as we transitioned our privacy model two years ago, have often overshadowed much of the good work we’ve done” (par. 5). This admission was hailed as a win for the Federal Trade Commission and the billion or so Facebook users. It also resulted in a complex consent agreement.

Facebook settled the case and agreed to 20 years of third party oversight of its Privacy Policy. Larry Magid of the Huffington Post assesses what this means for the end user: “In theory, what this should mean to consumers is that they can rely on information about privacy from Facebook as being accurate and complete. It should also mean that the information will be presented clearly and in language that the average person can easily understand” (2011, par. 8).

Still, users must “read” the Privacy Policy instead of just clicking “Agree” to fully understand what is public and what is private when they share anything on Facebook or make a Facebook post. For example, many users in June 2012 thought they would have the opportunity to vote on Facebook’s new Privacy Policy. Even the *Los Angeles Times* ran an article on how to “Have your say on Facebook privacy policy” with information on where and how to vote. However, the author, Michelle Maltais, also reveals that in the Facebook Privacy Policy fine print it states the vote is only “advisory” and about “270,000,000 users need to vote for it to stick” (2012, par. 4). The Privacy Policy is revised and renamed, but the user still has the responsibility to be vigilant.

Additionally, Facebook has added two recent updates and documents that users need to understand: the Data Use Policy and the Statements of Rights and Responsibilities. Both of these updates directly concern the end users privacy and went in to effect Nov. 15, 2013. The new changes to the Data Use Policy now clearly state to the user that Facebook can use profile pictures, location and other personal information in advertising. Some critics see the changes as an inappropriate expansion of the data and information Facebook collects from users (Tsukayama, 2013). These recent changes have prompted comments from the government. Tsukayama notes, Sen. Edward J. Markey has weighed in to criticize the changes: “Corporations like Facebook should not be profiting from the personal and sensitive information of children and teens, and parents and teens should have the right to control their personal information online.” However, Chief privacy officer Erin Egan explains Facebook’s updates as helping the user, “We simplified the explanation for how we receive information and clarified the types of information we receive when you use or run Facebook, including from your devices, such as your IP address or mobile phone number” (Egan, 2013). Facebook contends that privacy changes are directly aligned with the company’s values.

Facebook also acknowledges that the changes are in compliance with the FTC ruling in the newly updates Statement of Rights and Responsibilities: “As part of a legal settlement, we agreed to further explain how we may use your name, profile picture, content and information in connection with ads or commercial content. We included an example of how these ads work and explained that when you limit your audience, we’ll respect that choice” (Section-by Section Summary of Updates, 2013). Hence, users now bear the responsibility of controlling what will and will not be used of their personal information in Facebook advertising.

II. Understanding Facebook’s Values

Facebook’s Privacy Policy is a result of several professional values the company established. Three values that seemed to have shaped the Privacy Policy and its evolution are firstness, impact, and the public’s right to know. Each of these values affected changes in policy and impacted the company and all Facebook users, and users should be aware of their impact on the governing documents guiding Facebook’s current use of information.

Facebook arguably is valued greatly for its firstness. It was the first social network to enable users to communicate, share photos and updates through applications accessible from a free account that also required users to give their true identity. It also was the first to provide optional settings and the ability to join groups. The simplicity of the first privacy policy was in line with the simplicity of the application. Early users of The Facebook had to actively visit friends’ profiles to see posts.

One of the biggest changes to Facebook came on September 5, 2006 with the first launch of News feed (Cashmore, 2006). News Feed automatically provided passive streams of news and updates about friends. However, not all users liked having their information streamed.

Within two days of launching the group “Students against Facebook News Feed”, “the group

had 750,000 members-nearly 10% of Facebook's entire userbase (Parr, 2010). This created an immediate need for Facebook to assess its impact and privacy values, and the 2006

Facebook Privacy Policy was the result.

On Sept. 8, 2006, Mark Zuckerberg published an open letter to address the impact and the public's right to know. He started the letter: "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. I'd like to try to correct those errors now" (Open Letter, 2006). Facebook continued to make changes to its Privacy Policy and attempted to provide information through posts to users and "The Facebook Blog" in an attempt to keep the public informed and provide some information of the impact of the privacy changes.

The moral values of Facebook's Privacy Policy are considerably more complex than the professional. Evaluation the values of truthtelling and stewardship produce mixed results depending on the sources. Many sources revealed the 20-something CEO seemed sincere and honest when acknowledging the early mistakes of Facebook and privacy. However, as Facebook's profits grew, so did its exploitation of user data. The infographic, "A World More Transparent" demonstrates the shift of personal data from private to public (Freeman, 2012).

The infographic uses color-coding to demonstrate which portions of a user's page went from private to public from 2004 to present. Most critics of the changes argue that Facebook did not adequately inform users of the impact of the changes or provide enough information to fulfill the public's right to now.



Facebook continues to pursue its firsts, and there is evidence that many users are still unaware of the changes and impact. For example, in 2012 the Facebook Privacy Policy was renamed the Facebook Data Use Policy (Facebook, 2011). Another significant change was the assignment of a Facebook email June 25, 2012 (Hu, 2012). These current changes as well as the past admission of mistakes may cause many users to question Facebook's moral values concerning impact and public's right to know.

The Federal Trade Commission case may force Facebook to better address the values of justice and stewardship. The consent agreement requires Facebook to take several steps "to make sure it lives up to its promises". These steps include providing clear and prominent notices of changes. It also includes obtaining user consent before sharing information beyond the user's privacy settings (FTC File No. 092 3184, 2011, November 29).

Zuckerberg has made several changes to provide enhanced stewardship. These changes include hiring hackers to prevent security violations and obtaining third party audits that demonstrate Facebook has a privacy program in place that ensures the privacy of information is protected (Duell, 2011).

The Federal Trade Commission clearly demonstrated a commitment to the value of justice by holding Facebook accountable to the end user. The Federal Trade Commission held Facebook accountable for the promises the company made to consumers concerning personal information. It also demonstrated that companies must require opt-in consent for material changes to privacy. The legal settlement is consistent with the order imposed on Google and demonstrates a fair application of privacy priorities (FTC File No. 092 3184, 2011, Nov. 29).

III. Safeguarding Yourself on Facebook

Facebook users need to be vigilant in protecting their privacy. Many individuals and groups have, and several have been helpful in alerting others. In 2004, the Facebook group “Students against Facebook News Feed” received immediate attention when it alerted members about the implementation of news feed. Facebook also maintains a policy that allows users to put issues raised by comments to a vote, but many users ignore these posts (Dent, 2012). Facebook currently offers eight unique methods to improve your personal security. Users should understand what each of these eight security settings due and adjust them for individual preferences.

1. **Secure Browsing:** Enabling secure browsing alerts the user if he is using Facebook on an unsecured network. When on a secure network, Facebook will encrypt user activity making it harder for anyone else to access information.
2. **Login Notifications:** Login notification is an important step in securing user information. When enabled, Facebook will email or text a user when a user’s Facebook account is accessed from a device that has not been used before.
3. **Login Approvals:** Login approvals are very similar to the site keys used by banks and other online financial sites. When enabled, logging in to Facebook requires a security code that is sent to a phone or mobile device when a user attempts to log in from an unknown browser.
4. **Code Generator:** Code Generator is enabled when you require log in approvals. It generates a unique code every 30 seconds and each time you log in to Facebook.
5. **Apps Passwords:** (Enable when using log in approvals.) Some Facebook apps cannot receive security codes, so you may be locked out of the app. Apps passwords provide a secure way to log in to apps such a Jabber, Skype an Xbox.

6. **Trusted Contacts:** Trusted Contacts provides a safety net of friends that can securely help you if you ever are locked out of your account or if your account is high-jacked.
7. **Recognized Devices:** It is important to review and identify recognized devices. A list of the number, time location and type of device is kept for all Facebook sessions. Users can remove unfamiliar or casually used devices, such as computers in public places.
8. **Active Sessions:** Active Sessions provides recent accounts Facebook accounts are accessed. The session description includes date, location and the device used to access the account.

Reviewing these eight basic security features can help users maintain privacy and protect personal information. Facebook does provide users with reasonable control over security settings. However, most critics agree Facebook does not allow users as much control over privacy. Specifically, as soon as you select Privacy, Facebook alerts users, “your name, profile picture, cover photo, gender, networks, username and user id are always publicly available” (Privacy App Settings, 2013). This is because this information can help generate ad revenue for Facebook.

It is no secret that Facebook uses users to make money. As Julia Boorstin of MSN Money notes, “The social networks biggest asset is its user base” (2012). Advertisers want access to the millions of users posting comments and likes every day. In 2011, Facebook posted ad revenues of \$3.7 billion. Ad revenue also accounts for 82 percent of all first quarter revenue this year. Facebook also makes money from user transactions. Users use credit cards for games like Zynga’s Farmville, and Facebook takes 30 percent of the transaction. So, the more information

Facebook can provide to a potential advertiser, the more likely the company is to purchase more ad space. However, there are several areas where users do control their privacy.

Users always have control of posts. Users choose the audience for each, every, and all, Facebook posts. However, this does not mean people cannot find, view and share your posts. Hence, users should follow some basic advice to help keep private information private:

1. Only friend people you know and trust. However, this does not mean they cannot repost or share your posts.
2. Limit the personal information you share on Facebook; especially with companies and applications.
3. Monitor and control your post options. In 2013, Facebook ended the option for users to limit who could find them in graph search. However, users can limit posts and who sees the information on a news feed to Friends or Custom group settings.
4. Restrict contact options. This can help protect users from phishing scams and unwanted friend requests.
5. Limit past posts: Simply by clicking “Limit Past Posts” and agreeing to the prompt, users can change all past posts to the Friends Only view (Inside Facebook, 2013).

IV. Conclusion

The Federal Trade Commission consent settlement with Facebook is a clear attempt to assert personal privacy is important and companies need to establish policies to protect it. Facebook is demonstrating a concern for its citizenry by providing users with increased notifications and clear communication. However, with the vast amount of ways data are shared, Facebook will continue to have its policies challenged, and will continue to update the policies to

align with the company values, as well as, to help generate revenue. Hence, users need to be aware of the history of the privacy settings, monitor privacy and security settings and be sure to maintain a safe method to address privacy concerns while still enjoying the benefits of Facebook.

References

- Boorstin, J. (2012, May 17). Inside Facebook's money machine. *MSN Money*, Retrieved June 26, 2012, from
<http://money.msn.com/technology-investment/post.aspx?post=869a1b6c-0bb7-47b3-ac0a-25d10f6a5404>
- Cashmore, P. (2006). Facebook's facelift. *Mashable*, 9(5), Retrieved from
<http://mashable.com/2006/09/05/facebook-facelift-mini-feeds-and-news-feeds/>
- Christians, C. et al (2012). *Media ethics: cases and moral reasoning*. 9th ed. Boston: Pearson. Print.
- Constine, J. (n.d.). Facebook Fleshes Out Privacy Policy To Comply With Data Protection Audits, Will Hold Q&A On Monday. *TechCrunch*. Retrieved July 20, 2012, from
<http://techcrunch.com/2012/05/11/facebook-privacy-policy-changes/>
- Dent, S. (2012, 06 02). [Web log message]. Retrieved from July 5, 2012,
<http://www.engadget.com/2012/06/02/facebook-privacy-changes-vote-our-policy/>
- Doctorow, C. (2012, April 29). Timeline of Facebook privacy policy: from reasonable (2005) to apocalyptic (2010). *Boing Boing*. Retrieved July 8, 2012, from
<http://boingboing.net/2010/04/29/timeline-of-facebook.html>
- Duell, M. (2011, 12 7). Mark zuckerberg's private facebook photos revealed. *Mail Online*. Retrieved July 4, 2012, from <http://www.dailymail.co.uk/news/article-2070749/Facebook-security-glitch-reveals-Mark-Zuckerbergs-private-photos.htm>
- Egan, E. (n.d.). Proposed Updates to our Governing Documents. *Proposed Updates to our Governing Documents*. Retrieved November 27, 2013, from
<http://www.facebook.com/notes/facebook-site-governance/proposed-updates-to-our-governing-documents/10153167395945301>
- Facebook. (2011, Sept 23). *Facebook*. Retrieved June 28, 2012, from
<http://www.facebook.com/about/privacy/>
- Freeman, K. (2012). *Facebook privacy: Infographic*. (05 ed., Vol. 14). Retrieved from
<http://mashable.com/2012/05/14/privacywatch-infographic/>
- FTC File No. 092 3184, 2011. (2011, November 29).
<http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf>. Retrieved July 11, 2012, from ftc.gov/os/caselist/0923184/111129facebookagree.pdf
- Hu, E. (2012, June 25). [Web log message]. Retrieved June 28, 2012, from
<http://www.npr.org/blogs/alltechconsidered/2012/06/25/155735322/facebook->

- Improve Your Experience. (n.d.). *Improve Your Experience. Facebook*. Retrieved July 18, 2012, from <http://www.facebook.com/about/privacy/>
- Jones, H., & Soltren, J. (2005, December 14). *Facebook Threats to Privacy*. Retrieved July 10, 2012, from groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf
- Jr., J. P. (n.d.). Facebook Hit with Lawsuit Alleging Privacy Wrongs. *Reviews and News on Tech Products, Software and Downloads. PCWorld*. Retrieved July 22, 2012, from http://www.pcworld.com/article/255803/facebook_hit_with_lawsuit_alleging_privacy_wrongs.html
- Kirkpatrick, M. (2010, January 09). *Read write web*. Retrieved from http://www.readwriteweb.com/archives/facebook_zuckerberg_says_the_age_of_privacy_is_over.php
- Maltais, M. (n.d.). Have your say on Facebook privacy policy - latimes.com. *Los Angeles Times - California, national and world news - latimes.com*. Retrieved July 20, 2012, from <http://www.latimes.com/business/technology/la-fi-tn-facebook-privacy-public-vote-20120601,0,7362858.story>
- Opshal, K. (2010, April 28). *Facebook's Eroding Privacy Policy*. Retrieved July 14, 2012, from <https://www.eff.org/deeplinks/2010/04/facebook-timeline/>
- Parr, B. (2010). *An inside look at facebook's first privacy fiasco*. (07 ed., Vol. 21). Retrieved from <http://mashable.com/2010/07/21/my-facebook-story/>
- Patel, N. (n.d.). Facebook agrees to 20 years of privacy policy assessments to settle FTC lawsuit. *The Verge*. Retrieved July 22, 2012, from <http://www.theverge.com/2011/11/29/2596708/facebook-ftc-settlement-privacy-lawsuit>
- Protalinski, E. (n.d.). Facebook faces nationwide class action tracking cookie lawsuit. *ZDNet. Technology News, Analysis, Comments and Product Reviews for IT Professionals*. Retrieved July 22, 2012, from <http://www.zdnet.com/blog/facebook/facebook-faces-nationwide-class-action-tracking-cookie-lawsuit/9747>
- Quirk, M. B. (n.d.). Facebook's policy changes will mean your content can be used in ads if you use Facebook. *Consumerist*. Retrieved November 20, 2013, from <http://consumerist.com/2013/08/29/facebook-policy-changes-will-mean-your-content-can-be-used-in-ads-if-you-use-facebook/>
- R. v. Duarte*, [1990] 1 scr 30. (January, 25, 1990). Retrieved from <http://www.canlii.org/en/ca/scc/doc/1990/1990canlii150/1990canlii150.htm>

- Rashid, F. Y. (n.d.). Facebook Rejects User Input on New Privacy Policy. *Security Watch*. Retrieved July 22, 2012, from <http://securitywatch.pcmag.com/privacy/298965-facebook-rejects-user-input-on-new-privacy-policy>
- Section-by-Section Summary of Updates. (n.d.). *Section-by-Section Summary of Updates*. Retrieved November 26, 2013, from <https://www.facebook.com/notes/facebook-site-governance/section-by-section-summary-of-updates/10153200989785301>
- Senators' letter to Facebook. *Politico.com*, 27 April 2010. Web, 14 July 2012, from <http://www.politico.com/news/stories/0410/3640>
- Tsukayama, H. (2013, November 16). Facebook makes changes to its data use policies. *Washington Post*. Retrieved November 23, 2013, from http://www.washingtonpost.com/business/technology/facebook-makes-changes-to-its-data-use-policies/2013/11/15/0107eab4-4e2f-11e3-be6b-d3d28122e6d4_story.html
- Zuckerberg, M. (2006, September 8). [Web log message]. Retrieved from <https://blog.facebook.com/blog.php?post=2208562130>
- Zuckerberg, M. (2011, November 29). [Web log message]. Retrieved from <https://blog.facebook.com/blog.php?post=10150378701937131>
- 5 steps to protect your Facebook privacy in lieu of upcoming Graph Search changes - Inside Facebook. (n.d.). *Inside Facebook*. Retrieved November 26, 2013, from <http://www.insidefacebook.com/2013/10/22/how-to-protect-your-facebook-privacy-in-lieu-of-graph-search-privacy-changes/>