Facebook, Beacon and Your Privacy

By Katherine Blizard

CSC 300: Professional Responsibilities

Dr. Clark Turner

March 2, 2011

Abstract

In late 2007, Facebook launched a platform with affiliates in order to allow Facebook users to publish their activities with Facebook's affiliates. This service, called Beacon, allowed web surfers on affiliate websites to load a pop up directly from Facebook. But, Beacon sent data to Facebook regardless if a user selected "No, thanks" to a prompt, and gathered the data of people who were not Facebook users at all. For one user, Sean Lane, this lead to an expensive Christmas present purchased for his wife on Overstock.com being broadcast to all of his friends, including his wife. This report analyzes if Facebook's use of Beacon was ethical according to the ACM/IEEE code of ethics. Facebook had created Beacon at the expense of the privacy of it's users, making it unethical.

Contents

1 Facts

1.1 Facebook

"Facebook helps you connect and share with the people in your life.[1]"

Facebook runs a social networking service at http://www.facebook.com. Internet users sign up to Facebook to connect to their contacts (known as "friends") to exchange information between them. When a Facebook user friends a person, they get to see information about the activities of that person pushed to their news feed. The news feed then is the collective aggregation of the updates of all that user's friends. [31, p. 19-20] [1]

Facebook provides advanced privacy settings for its users. The privacy settings consists of a long checklist of individual parts of the user's profile that they can choose to show to their friends or push to their news feed. [1]. However, Facebook does not direct users to their privacy settings as they log into the website. They would have had to navigate themselves to the privacy settings page and interpret 2,283 words before knowing that their profile was set up correctly. [31, p. 23] [29] Furthermore, Facebook's Privacy Policy only applied to action taken or cookie originating on www.facebook.com, not on the Beacon affiliated websites [31, p. 23-25].

1.2 Beacon

On November 6th, 2007, Facebook launched a new feature on it's social networking service named Beacon. Beacon was a service that was placed as an iFrame onto the web pages of Facebook Beacon's Activated Affiliates, known from here on as Beacon's affiliates. The affiliates are each a third party website to Facebook and include businesses like Blockbuster and Overstock.com. When a person performs an action on an affiliate website, such as purchasing an item, rating a video or playing a game, the Beacon iFrame embedded in the page activated and loaded a pop-up directly from Facebook.com. The pop-up told the user that Beacon was sending information to Facebook and gave them an option to click "No thanks" to prevent the information from showing up in their profile. The pop-up disappeared after about 10 seconds if the user did not respond to it. [31, p. 23-27] [23]

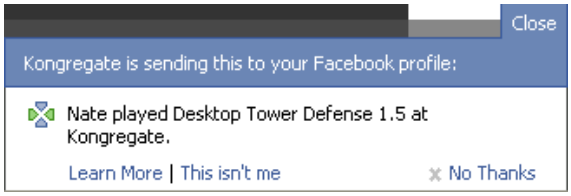

Figure 1. The Beacon pop-up [48]

Interestingly, the pop up would not give the affiliate user a choice on whether or not the information Beacon took was sent to Facebook. The iFrame sent the data straight the Facebook.com whether or not a user pressed "No thanks." The only thing the button did was prevent Facebook from publicly publishing it to any news feeds. Furthermore, the iFrame still activated for affiliate users who did not sign up for Facebook, or deliberately logged out of Facebook. In that case, the iFrame loaded an invisible pop up that the affiliate user would never see, and then sent the data to Facebook anyway [23] [35].

Many Facebook users disliked the Beacon service[43]. Since Beacon was activated

and opt-in by default, Facebook users had to manually opt-out of each of Beacon's 44 affiliates in order to prevent its effects. There was no easy option for users to turn Beacon off permanently or automatically opt-out of any future possible affiliates added to the program. In other words, to keep out of Beacon, Facebook users must continually watch for new Beacon affiliates and opt-out of each of them [40][31].

1.3 Class Action Lawsuit

Before Christmas 2007, Sean Lane went online shopping at Overstock.com to buy some jewelry for his wife. Unaware to him, Beacon took information about his purchase and published it to his Facebook news feed, mentioning the 51 percent discount. All of his friends, including his wife, saw that he had bought a ring. His wife then texted him on his phone, inquiring "Who is this ring for?"[35]. Later in 2008, Sean Lane and other Facebook users would file a class action suit against Facebook and their Beacon affiliates. [35] [31, p. 6]

2 Research Question

Was Facebook acting ethically with their use of the Beacon program?

The software that Facebook writes, like Beacon, ethically impacts the millions of users it has [18]. Since the main focus of this question will rest on how Beacon handled user data given to it, the answer will focus on the privacy issues surrounding Beacon. The answer to this question will reveal the manner in which software engineers might better approach the issue of privacy of end users.

3 Arguments For

It is ethical for Facebook to design the Beacon service the way they did:

3.1 Facebook, at Beacon's launch

Before they changed their mind from the onslaught of negative press [42], Facebook in a press release mentioned that they had advanced privacy options for their users. In their eyes the amount of privacy options already available at the time was adequate enough to launch Beacon. [4]

3.2 Chamath Palihapitiya, Facebook VP of marketing and operations

After Beacon became controversial, Vice President Palihapitiya made some comments to the New York Times. Beacon was designed to be lightweight and allow users to sample its varied capabilities. Since Beacon behaves differently on different websites, users should be able to turn off Beacon on a per-site basis. Having to opt-in to them all would not be as lightweight. Furthermore, Facebook should listen to feedback from its userbase, and most of the complaints about Beacon are originating from the press. The press is not representative of Facebook users. [45]

3.3 Wired article commenters

In short, if one does not like Facebook, they do not have to use Facebook. Facebook is a free service that is not necessarily important in the large scheme to its users, and its creators have a right to make a profit from their work. Facebook users understand

that they use Facebook for free and should expect Facebook to try and make a profit. Also, there are alternatives to Facebook in terms in communicating with people. It is not difficult for a dissatisfied Facebook user to deactivate their account and move to alternatives. [42]

4 Arguments Against

It was not ethical for Facebook to use Beacon in a way that disregards the privacy of its users:

4.1 Sean Lane and the plaintiffs of the class action lawsuit

Facebook and Beacon tracked Facebook non-users and Facebook users after they had logged off, making Beacon a deceptive application. Beacon was inadequate, untimely and uninformative because the user often did not see the timed pop-up prompt before it disappeared. Beacon was misleading because the user was led to believe they had control over whether their information was sent to Facebook or not. [31, p. 28]

4.2 Mike Rogers, editor and publisher of PageOneQ

PageOneQ is a website geared toward homosexual people, and teaches the youth to avoid sharing their information freely on the Internet. Beacon's disregard of privacy can potentially expose secrets that place Facebook users in danger, such as "the possibility that the youth could be outed and harassed as a result." [35]

5 Analysis

Software is "the programs used to direct the operation of a computer [11]." Facebook develops software for their online social networking services. Since Beacon lived on third party sites that directed how the operation of that web page (which lived, after some abstraction, on the computer), it is fitting to refer to Beacon as software. This section will focus on how the ACM/IEEE Software Engineering Code of Ethics and Professional Practice (the SE code) can be applied to Facebook's use of Beacon, since they hire software engineers[10]. This section will also apply various other ethical systems to Beacon's design to determine whether it was ethical in those places.

In order to apply the SE code to Beacon's predicament, it is necessary to clarify of some of the terms in the original tenets. It is Facebook that developed Beacon, and Beacon is the specific piece of software that this research question refers to. So, Facebook and Beacon will refer to the software engineers and the software, respectively. This translation of the engineers and the software will apply to all of the tenets analyzed in this paper.

5.1 Authorization: SE Code 3.13

The Software Engineering code of ethics has a tenet concerned about the data used in software. Ultimately, Beacon is a piece of software that takes data from users and sends it to Facebook. The analysis begins by looking at Beacon's fundamental functionality: how it takes data from users.

5.1.1 Transformation of the Tenet

> **Original SE Code Tenet:** 3.13. [*Professional software engineers* shall, as appropriate] *Be careful* to use only *accurate data* derived by ethical and lawful means, and use it only in *ways properly authorized*. [20]

The crux of this tenet asks what does accurate data mean, what does it mean to derive it, and who authorizes it? The data that is being handled by Beacon and Facebook originated from the users of the affiliate sites. So that data is the data that is being referred to by the tenet in this instance.

Both of the words "ethical" and "lawful" are words with complicated domains. The ethical argument will form as Beacon is analyzed in this document. As for legality, Sean Lane et. al sued Facebook and the Beacon affiliates for violating 5 laws, but settled out of court instead of reaching a conclusion. [5]

Instead, this part of the analysis will focus on who authorizes the data and whether or not taking the data was truly authorized. The dictionary definition of authorization is "duly sanctioned.[13]" Sanctioning then means, "to authorize, approve, or allow.[17]." But, a problem appears when looking at that word, "allow." It has several meanings: one meaning is "to permit by neglect," and the other meaning is "to give permission to or for[12]." Essentially, one definition only refers for opt-in systems, and the other can refer to opt-out systems like Beacon. The 'permission' definition appears in several of these definitions, so it feels the most obvious. But, since 'allowed' is the most ambiguous term in the definition of sanctioning and since Beacon is an opt-out system, it will be the word of focus. For completeness sake, the analysis of authorization will have to examine both interpretations of allowance.

Replacing the original tenet with the new terms results in the following.

> **Domain-Specific SE Code Transformation:** [*Facebook* shall, as appropriate] *collect only with allowanceBeacon affiliate user data...* and use it only in ways *affiliate website users have allowed*.

5.1.2 Did Affiliate Users Authorize Use of Their Data?

When a person signs up to become a Facebook user, they intend to give Facebook the privilege of handling the information on the terms of Facebook's privacy policy [6]. Otherwise, people who do not agree to the terms in the privacy policy do not become Facebook users. However, the privacy policy on Facebook did not cover actions taken outside of www.facebook.com [31, p. 23-25]. This means that actions taken on the Beacon affiliate websites aren't covered by the Facebook privacy policy.

The Beacon pop-up that is activated by the iFrame disappears automatically after about ten seconds. A user who was distracted by something like a phone call may not come back soon enough to read the pop up. But, Facebook will post the data to the news feed unless the user presses the "No thanks" button. [31, p. 23-27] [23]. Even a well informed user that read the privacy policy may end up with their data taken without their knowledge. If a user does not consciously press "No thanks," Facebook is

collecting data that it is not authorized to collect.

However, this can change if the neglectful definition of "allow" is in effect. If that definition were to be considered, then the next step is to determine whether the Facebook users are excused of the responsibility to neglect something. Otherwise, Facebook was reasonable in designing Beacon to treat an opt-out system as a proper authorization.

It is not reasonable to make the case that a person is responsible for everything that transpires in this universe. The dictionary says that responsibility relates to "accountability" or "as for something within one's power[11]". In order for a Facebook user to properly allow their data to be used, they would have to have some sort of power over the situation. Otherwise, they don't have the responsibility to allow or neglect it. An affiliate user would not have any power over the situation when Beacon took their user data without giving them an option to disallow it.

Within a month after Beacon first released, Stefan Berteau analyzed the internet traffic that left his computer when Beacon activated. Deliberately selecting "No thanks," Berteau found that the WireShark packet analyzer found that his data was sent to Facebook regardless that he explicitly pressed the button. Berteau was more surprised when he logged out of Facebook, restarted his browser, returned to the same affiliate website and found that Facebook had also silently collected the data from that transaction [23]. In both cases, the data was sent to Facebook before the iFrame (invisible or not) loaded the pop-up. [23] Facebook had never truly given the user an opportunity to give permission to send their data. In the case of users that were logged out, their data was taken without being notified, much less with explicit notice or authentication. [23] [31]

Since Facebook did not have an agreement with the affiliate users in their privacy policy, and because Facebook took user data without giving the user any control, Facebook did not collect affiliate user data with proper allowance. Beacon's use was in violation of SE Code 3.13.

5.2 Deception: SE Code 1.06

5.2.1 Transformation of the Tenet

In the analysis about Beacon's authorization techniques, a possibility came up that users may not be aware that Beacon was taking their data without permission. This was an issue that was brought up in Sean Lane's case [31]. It is important that Facebook isn't using Beacon deceptively because deception is against the deontological principle of honesty [3]. This point also exists in the Software Engineering Code.

> **Original SE Code Tenet:** 3.12. [*Professional software engineers* shall, as appropriate] Be fair and *avoid deception* in all statements, particularly public ones, *concerning software or related documents, methods and tools*. [20]

Deception is the "act of deceiving." Deceiving, or misleading, is to "to lead into error of conduct, thought, or judgment[11]." What this means is that Beacon must not lead users to think Beacon is doing one thing

when in actuality Beacon is doing something else entirely.

The tenet for this case now looks like:

> **Domain-Specific SE Code Transformation:** [*Facebook* shall, as appropriate] Be fair and *not mislead users into making erroneous thoughts or judgments* in all statements ... *concerning Beacon and the data it is handling.*

5.2.2 Misleading Thoughts

When Beacon's pop-up activated for an affiliate user, there was the statement "[Affiliate name] is sending this to your Facebook profile[48]" with a button in the lower right saying "No thanks."

What turned out to be the case was that the "No thanks" button was asking for permission to post the new bulletin as a news feed. But the header text on the Beacon pop-up says "sending this[48]." This implies that the pop-up was asking for permission to send the data to Facebook, when it was really asking about posting it to the news feed. As established in the previous section, the user actually had no choice to send that data to Facebook [23].

On account that the user was led to believe that they had power to decide whether they could send their data, Facebook misled its users into making erroneous thoughts and judgments. Facebook's use of Beacon was in violation SE Code 1.06.

5.3 Respecting Privacy: SE Code 3.12

5.3.1 Transformation of the Tenet

This part of the SE code deals with the realm of privacy. This part of the analysis will observe the impacts Facebook, Beacon, and the feed posts Beacon generates from user data. The general case of the SE code tenet is the one below. The tenet will have to be changed to a more domain-specific version in order to analyze Beacon though it.

> **Original SE Code Tenet:** 3.12. [*Professional software engineers* shall, as appropriate] Work to develop *software* and *related documents* that *respect the privacy* of *those who will be affected* by *that software*. [20]

Dictionary.com defines one kind of document as "a computer data file[14]." They also define a computer file as "a collection of related data or program records stored on some input/output or auxiliary storage medium [15]." Beacon generates posts made of user data that are stored on Facebook and pushed to Facebook's news feed[6], [31]. Those feed posts therefore count as related documents to Beacon.

Furthermore, it is the users who are browsing affiliate websites that trigger the Beacon actions. Beacon is handling the data of the users who triggered it; therefore, the affiliate site users are the people who are affected by the software [31] [23].

Privacy can be "the state of being free from intrusion or disturbance in one's private life or affairs" and it can also be simply defined as "secrecy"[16]. Substituting the

more precise terms back into the tenet, we again look at the transformed tenet that this analysis will examine.

> **Domain-Specific SE Code Transformation:** [*Facebook* shall, as appropriate] Work to develop *Beacon* and *related feed posts without revealing secrets* or *intruding in the affairs* of *all affiliate website users affected* by *Beacon*.

5.3.2 The Secrets of Facebook Users

By the Software Engineering Code, Facebook and Beacon are obligated to keep the secrets of Facebook users. Secrets are things that are "kept from the knowledge of any but the *initiated or privileged* [11]." The right to privacy that this part of the SE code refers to is a right to *choose* who one's information is shared with and to what extent, timing and manner it is shared [49, p. 12]. In other words, it is the right of the Facebook user to choose who the privileged recipients of their messages are, including their friends on Facebook. In this case, Facebook would be a middleman between the user and his or her friends.

Facebook then must forward the user's new posts only to that user's privileged friends. There are several points in time where the user's choice matters: First, where the user authorizes Facebook to take data from them and put it on the news feed, and secondly, selecting who gets to see the data that Facebook forwards to the news feed. Fortunately, Facebook has advanced privacy settings that allow the user to define which users can see new posts by default[4][1]. This gives some users some control over who gets to see the posts after Facebook puts them onto the news feed.

Yet, Facebook must be authorized to put the information on the news feed in the first place. If Facebook was not authorized to put the user's data into the news feed, then it means that the user did not choose to share that information with their friends. We have already determined in the last section that the data Beacon took was not authorized [23][31]. Beacon placed those unauthorized posts onto the news feed where other users could see them, like Sean Lane's friends. On account that the affiliate user did not choose which of his Facebook friends were priviledged enough to view that data, unpriviledged people like Sean Lane's wife would have seen that data[35][31].

In other words, taking the data from the affiliate websites was at least a breach in authorization. Posting the unauthorized data on the news feed was a breach in privacy.

This happened to Sean Lane when he bought the ring from Overstock.com. He was keeping the ring as a holiday secret from his wife when Beacon spoiled the surprise though the news feed. Since Sean Lane did not see the Beacon pop-up prompt, his data was not authorized to be sent to Facebook. Facebook displayed the feed post to his wife without his permission. [35] Facebook did not respect his privacy when they revealed his secrets, so Facebook was in violation of SE Code 3.12.

Figure 2. The privacy setting moderating new posts [1]

5.4 Diminishing Quality of Life: SE Code 1.03

5.4.1 Transformation of the Tenet

The fourth tenet of the SE code to be analyzed is number 1.03. This tenet will be used to analyze the relation of Facebook, Beacon and the quality of life of Facebook users that encountered Beacon.

> **Original SE Code Tenet:** 1.03. [*software engineers* shall, as appropriate] Approve *software* only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not *diminish quality of life*, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good. [20]

Determining what "Quality of Life" means would have been difficult it it weren't for the Quality of Life Research Unit at Toronto University. They define quality of life simply as "The degree to which a person enjoys the important possibilities of his or her life." To achieve the important possibilities in life, a person must realize the concepts of being (who one is), belonging (connections with one's environments), and becoming (achieving personal goals, hopes, and aspirations). The specific tenets of the Quality of Life Model that may apply to Beacon are as follows: [38]

1. Physical being; health
2. Psychological Being; self-esteem, self-concept and self-control
3. Social Belonging; family, friends, neighborhood, community, and intimate others
4. Community Belonging; employment

For Beacon to be an ethically designed system, it should not diminish any of those tenets of the quality of life of the Facebook users.

Beacon also must not diminish privacy of the Facebook users, but we have already established that this was not the case.

With these more specific interpretations of the original tenet, the transformed SE code tenet looks like this:

> **Domain-Specific SE Code Transformation:** 1.03: [*Facebook* shall, as appropriate] Approve *Beacon* only if they have a well-founded belief that it ... does not *does not harm the physical/psychological being or the social/community belonging of Facebook users...* [20]

5.4.2 Being and Belonging

Facebook should not directly jeopardize a user's role in their social life and in their communities. The way it can be jeopardized is when the community learns some information about that user that they do not

agree with. For instance, a user who makes a slight social error may end up as an example on websites like Failbook[24]. But these reactions can range to a more severe form of punishment, such as when a Connecticut ambulance company fired an employee based on her negative comments on Facebook about her boss. While the National Labor Relations Board won a legal settlement in 2011 over this issue, it shows that information posted to Facebook can have negative repercussions on their users' lives. [30]. Furthermore, Facebook is an internationally accessible website and the legal systems of each country that can access it differs. [1] It is best left to the user's discretion to decide what information they should be sharing, rather than Facebook centralizing decisions that would have otherwise differed based on legal and cultural origins.

But since Beacon readily does not respect the user's privacy and shares the secrets of its users, there is no guarantee that Facebook will not jeopardize a user's role in their social life. The secrets that can be shared by Beacon can be like the secrets that led to the firing of the Connecticut ambulance employee. Plus, Beacon has the ability to show these secrets to hundreds of people, such as the hundreds of people who saw Sean Lane's gift purchase [35]. Furthermore, since the Beacon service takes the information of logged out users, there is no guarantee that the user that activated the Beacon trigger is the same person who owns the Facebook cookie [23] [31]. That can lead to someone else's secret being posted under the user's name.

The secrets that Beacon can spill can put some kinds of users in great danger. Nine out of ten LBGT teenage students face harassment, and nearly two-thirds of them feel that their safety is threatened at school [8]. Beacon could have revealed the orientation of a user by, for example, revealing a LBGT oriented movie that they rented [35]. Their social belonging, psychological being and even physical health could be at stake.

This means that Beacon was handling secrets in a way that can harm the being and belonging, and thus the quality of life, of Facebook users. Therefore, Facebook was in violation of SE tenet 1.03.

5.4.3 Beacon's Alternative Implementation

Concerning privacy, there is one detail that may be impossible for Facebook to solve. If Beacon was not deceptive and dealt with authorization appropriately, Beacon still may not satisfy all the user's privacy requirements. Most Facebook users would not read the privacy policy upon joining, assuming they could understand it in the first place [29, p.45]. Giving the users more advanced privacy controls would not help that much, either. That would make Facebook difficult to use and most users wouldn't want it[29, p.48-51]. The utilitarian ideal that all users will have their quality of life improved by Facebook may not be achievable.

But, it is not as useful to declare the whole of Facebook and Beacon unethical and demand that they close. If Facebook did not provide some sort of utility to its 300 million users, then those users would not find any value in Facebook [18] [34]. Also, Software Engineering code 3.08 states that "Ensure that specifications for software on which they work have been well documented, satisfy the users requirements and have the ap-

propriate approvals [20]." Eliminating any chance of a privacy breach by getting rid of Facebook would not meet the requirements of Facebook users, which could also be unethical. Similar services like Google's free gmail, which 170 million users used as of March 2010, provides a lot of utility to communicate in the online world [9]. If the argument were to be made that Facebook should be taken down due to a possibility that some users' privacy issues get them hurt, then the same arguments can take down services by Google, Yahoo, Microsoft and others. This would result in a loss of a lot of functionality to their services, and a loss of utility.

It is then up to the users to decide at their own risk what they should share on Facebook. Facebook can instead take up the deontological duty to be honest [3]. They can do so by honoring authorization and avoiding deception as the Software Engineering code says they should. If Facebook had implemented Beacon to observe those procedures correctly, Beacon would be ethical to use. In that case, Beacon would have been a service that allows its users to share only what they intended to share. Any decrease in the quality of life of a user would be as a result of their own decisions, not of the decisions a third party took for them.

However, the reality is that Beacon was deceptive and took user data without authorization. The result of this created a system that endangered the quality of life of Facebook users, so Facebook was still in violation of SE tenet 1.03.

5.5 Objectively, Should Facebook Care?

Ayn Rand, the woman who founded Objectivism, explains that the best moral system involves self-interest as it's highest goal. The core tenet of this part of Objectivism lies on it's constraints on what a rational human being is expected to do in society.

> Man—every man—is an end in himself, not the means to the ends of others. He must exist for his own sake, neither *sacrificing himself* to others nor *sacrificing others* to himself. The pursuit of his own rational self-interest and of his own happiness is the highest moral purpose of his life. - Ayn Rand[39]

Sacrificing something is "to surrender or give up, or permit injury or disadvantage to, for the sake of something else [11]". The two constraints regard someone being made to sacrifice themselves for someone else's good, or sacrificing other people for his or her own good. When looking at Beacon from Facebook's perspective, the answer of whether or not Facebook was acting ethically or not is not immediately clear. To make it clear, Facebook's actions will be filtered through the lens of sacrificing themselves. This lens will look at whether Facebook's actions through Beacon that can sacrifice Facebook itself in the long term.

5.5.1 Can History Do to Facebook What It Did to MySpace?

Before Facebook became popular, there were huge social networks like it. Notably, MyS-

pace was the dominant social network until Facebook came onto the scene. Michael J. Wolf, former MTV president who tried to buy Facebook said "These Internet businesses tend to have a cycle. Theres a lot of people who wonder if the same thing will happen to Facebook [21]." In recent years, millions of MySpace users have been leaving [21]. Marshall Kirkpatrick, writer at ReadWriteWeb, notes that "It's not a business problem that MySpace has, it's a core user experience problem[32]." If bad user experience inspired the exodus from MySpace to Facebook, then bad user experience can inspire another exodus from Facebook to a new competitor.

Objectively, Facebook losing its userbase would not be in its self interest. Yet, using Beacon to disregard the authorization and privacy needs of its users can create negative user experiences. The Beacon backlash from users after it launched shows shades of this[42]. Beacon is an example of sacrificing long term consequences for short term gains. If enough users are dissatisfied, a competitor can capitalize on this and become the next dominant social network.

In April 2010, an open source project named Diaspora was announced. Diaspora billed itself as "the privacy aware, personally controlled, do-it-all distributed open source social network [27]". The BBC referred to it as the "Anti-Facebook[44]." When it opened a donation channel in Kickstarter to ask for funds, the 10,000 dollar goal was met and surpassed within 12 days. As of this writing, Diaspora is still in development, but it is currently the fourth most watched and forked project on GitHub [19]. Diaspora took the sudden interest and popularity of its idea as an indication that privacy is a serious issue in social networks that isn't addressed by Facebook [27]. This is just one example of a competitor who is capitalizing on the faults of Facebook.

If Facebook wants to hang on to it's user base and maintain the best interests for itself, it should not sacrifice the privacy needs of its users for short term gains. They will have to proceed with their releases without causing so much backlash.

5.5.2 What Were They Thinking?

After the Beacon backlash, Facebook publicly apologized [42]. In their apology, Mark Zuckerberg vaguely described their thought process for creating Beacon.

> "When we first thought of Beacon, our goal was to build a simple product to let people share information across sites with their friends. It had to be lightweight so it wouldn't get in people's way as they browsed the web, but also clear enough so people would be able to easily control what they shared. We were excited about Beacon because we believe a lot of information people want to share isn't on Facebook, and if we found the right balance, Beacon would give people an easy and controlled way to share more of that information with their friends. But we missed the right balance." - Zuckerberg[50]

What Zuckerberg said about finding the right balance was in reference to Beacon's

specifications. Facebook had greatly misjudged what the user's requirements were, and did not catch their error until after Beacon had released. In the Chaos Report by the Standish Group, the number one reason cited for software projects becoming challenged was lack of user involvement. The leading causes of failed projects were incomplete requirements and lack of user involvement [2, p. 3-4]. The class action lawsuit and a petition signed by fifty thousand users are examples that show that the specification designers were not in touch with the users. [31] [46]. Facebook should have checked with the users the first time instead of using Beacon's release and response as an expensive bug report. They would have avoided having to apologize, they wouldn't have had to redesign the system as Facebook Connect, and they would have been on a faster track to fulfilling their interests [36].

As for the details of their design process, it is unknown. It is not known why Facebook did not consider their requirements carefully enough, and there are many ways that Facebook could have injured itself. They could have had a bad software design process that they didn't fake well enough, as David Parnas and Paul Clements describe in their article "A Rational Design Process [26]." Or, it could have been caused by an incompetent in a critical position at Facebook, as Dunning, Kruger, and Farrell-Vinay describe [25][28]. While a total analysis would feel incomplete, there is not enough information to take the analysis beyond mere speculation. Facebook will have to find and repair its own issues if it wants to further its own interests.

6 Conclusion

Facebook launched Beacon under the pretense that they understood what their users needed, but they were very far off their requirements target. Beacon was launched onto third party websites despite Facebook not having a privacy policy defined for third party sites. Beacon collected data from users who weren't logged in and despite that some users pressed "No thanks" to the pop-up prompt. In other words, Beacon was taking user data without authorization. Since Facebook users were expecting that pressing "No thanks" would prevent Facebook from collecting their data, Beacon was also deceptive.

As a consequence of misusing data, Beacon did not respect the privacy rights of its users. Beacon was sending data to the news feeds that contained secrets that people did not want their friends to see. For instance, when Sean Lane's Christmas gift was posted and his wife saw it. In exposing secrets in this fashion, Beacon might have exposed secrets that may have harmed the social belonging of Facebook users, and might have gotten some people harassed and hurt.

In violating the Software Engineering tenets 1.03, 1,06, 3.12, and 3.13, Facebook was unethical in their use of Beacon.

What Beacon brought Facebook was a landslide of criticism and negative press. People who are aware of Facebook's bad reputation with privacy are making alternatives to it, like Diaspora. Facebook could have avoided the debacle Beacon brought if they had only double checked their requirements with their users.

References

[1] "Facebook.com: Facebook's profile." [Online]. Available: http://www.facebook.com

[2] "The standish group report: Chaos," 1995.

[3] "Deontological ethics," November 2007. [Online]. Available: http://plato.stanford.edu/entries/ethics-deontological/

[4] "Leading websites offer facebook beacon for social distribution," November 2007. [Online]. Available: http://www.facebook.com/press/releases.php?p=9166

Facebook press release for Beacon

[5] "Settlement agreement," September 2009.

[6] "Facebooks privacy policy," December 2010. [Online]. Available: http://www.facebook.com/policy.php

[7] "Facebooks privacy policy," October 2010. [Online]. Available: http://www.facebook.com/terms.php

[8] "Nine out of ten lgbt teens students face harassment," September 2010. [Online]. Available: http://www.gayrva.com/2010/09/16/nine-out-of-ten-lgbt-teens-students-face-harassment/

[9] "Number of gmail users," March 2010. [Online]. Available: http://www.numberof.net/number-of-gmail-users/

[10] "Careers: Software engineering," Feburary 2011. [Online]. Available: http://www.facebook.com/careers/department.php?dept=engineering

listing of their open software engineering positions

[11] "Dictionary.com unabridged," Feb 2011. [Online]. Available: http://dictionary.reference.com

[12] "Dictionary.com unabridged: Allow," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/allow

[13] "Dictionary.com unabridged: Authorized," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/authorized

[14] "Dictionary.com unabridged: Document," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/document

[15] "Dictionary.com unabridged: File," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/file

[16] "Dictionary.com unabridged: Privacy," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/privacy

[17] "Dictionary.com unabridged: Sanctioned," Feb 2011. [Online]. Available: http://dictionary.reference.com/browse/sanctioned

[18] "Facebook factsheet," Feburary 2011. [Online]. Available: www.facebook.com/press/info.php?factsheet

[19] "Popular forked repositories," Feburary 2011. [Online]. Available: https://github.com/popular/forked

[20] "Acm/ieee-cs software engineering code of ethics and professional practice," ACM/IEEE. [Online]. Available: http://www.acm.org/about/se-code

sections 1.03, 3.12, 3.13

[21] T. Arango, "Hot social networking site cools as facebook grows," Janurary 2011. [Online]. Available: http://www.nytimes.com/2011/01/12/technology/internet/12myspace.html

[22] K. Bell, March 2011.

peer review

[23] S. Berteau, "Facebook's misrepresentation of beacon's threat to privacy: Tracking users who opt out or are not logged in," November 2007. [Online]. Available: http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logge aspx

[24] "Failbook: Too funny to unfriend," Cheezburger Network. [Online]. Available: http://failbook.failblog.org/

[25] J. K. David Dunning, "Unskilled and unaware: How difficulties in recognizing one's own incompetence lead to inflated self-assessments."

[26] P. C. David Parnas, "A rational design process: How and why to fake it," 1986.

[27] "Diaspora blog," Diaspora, Janurary 2011. [Online]. Available: http://blog.joindiaspora.com/2010/05/08/we-did-it.html

[28] P. Farrell-Vinay, "Process of incompetence."

[29] J. Grimmelmann, "Saving facebook," March 2009. [Online]. Available: http://www.law.uiowa.edu/journals/ilr/Issue%20PDFs/ILR_94-4_Grimmelmann.pdf

70 page report on Facebook's Privacy issues in general

[30] S. HANANEL, "Feds settle case of woman fired over facebook site," Feburary 2011. [Online]. Available: http://news.yahoo.com/s/ap/20110208/ap_on_re_us/us_facebook_firing

[31] A. Himmelfarb, "Class action complaint," August 2008. [Online]. Available: http://www.wired.com/images_blogs/threatlevel/files/facebook_beacon_complaint0812081.pdf

Legal complaint

[32] M. Kirkpatrick, "Myspace is dead - the internet is growing up," April 2009. [Online]. Available: http://www.readwriteweb.com/archives/myspace_is_dead_-_the_internet_is_growing_up.php

[33] B. Mathis, "How facebook is becoming the next myspace," June 2010. [Online]. Available: http://laptoplogic.com/resources/how-facebook-is-becoming-the-next-myspace

[34] J. S. Mill, "Utilitarianism," 1863. [Online]. Available: http://www.utilitarianism.com/mill1.htm

[35] E. Nakashima, "Feeling betrayed, facebook users force site to honor their privacy," November 2007. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503_pf.html

[36] N. O'Neill, "Facebook connect is facebook beacon redesigned," September 2008. [Online]. Available: http://www.allfacebook.com/facebook-connect-is-facebook-beacon-redesigned-2008-09

[37] J. C. Perez, "Facebook's beacon more intrusive than previously thought," November 2007. [Online]. Available: http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html

from PC World

[38] "The quality of life model," Quality of Life Research Unit, University of Toronto, Feburary 2011. [Online]. Available: http://www.utoronto.ca/qol/concepts.htm

[39] A. Rand, "Introducing objectivism," 1962. [Online]. Available: http://www.aynrand.org/site/PageServer?pagename=objectivism_intro

[40] D. Reisinger, "Facebook faces beacon class-action lawsuit," August 2008. [Online]. Available: http://mashable.com/2008/08/14/facebook-beacon-class-action-lawsuit/

[41] K. Scanlon, Feburary 2011.

peer review

[42] B. Schiffman, "Facebook ceo apologizes, lets users turn off beacon," Wired, December 2007. [Online]. Available: http://www.wired.com/techbiz/startups/news/2007/12/facebook_apology

[43] ——, "Facebook is always watching you," December 2007. [Online]. Available: http://www.wired.com/epicenter/2007/12/facebooks-is-al/

Details some of Beacon's intrusiveness

[44] M. Shiels, "The anti-facebook," BBC, May 2010. [Online]. Available: http://www.bbc.co.uk/blogs/thereporters/maggieshiels/2010/05/the_antifacebook.html

[45] B. Stone, "Facebook executive discusses beacon brouhaha," November 2007. [Online]. Available: http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/

[46] L. Story, "Facebook retreats on online tracking," November 2007. [Online]. Available: http://www.nytimes.com/2007/11/30/technology/30face.html

[47] C. Turner, March 2011.

peer review

[48] N. Weiner, "Block facebook beacon," Ideashower, November 2007. [Online]. Available: http://www.ideashower.com/blog/block-facebook-beacon/

[49] e. a. Yael Onn, Privacy in the Digital Environment. Haifa Center of Law and Technology, 2005.

definition on page 12. Description of privacy on pages 1-12

[50] M. Zuckerberg, "Thoughts on beacon," December 2007. [Online]. Available: http://blog.facebook.com/blog.php?post=7584397130