

**A CDD Report**  
**The Facebook Economy: Deficits in Data Privacy**  
**By: Adam Mayle**

In May 2007, Facebook launched Facebook Platform, which opened up the site to outside developers, granting them unprecedented access to its core functions and changing Facebook from a closed social network into an open business forum.<sup>1</sup> The calculus behind this decision was simple: in exchange for allowing developers extraordinary access to Facebook's then twenty six million users,<sup>2</sup> Facebook would become a richer social environment, attract more users and improve its "social graph," the network of connections and relationships between its members.<sup>3</sup> As Facebook founder Mark Zuckerberg stated at the time, "the Facebook platform is optimized for building applications in Facebook, and with more value for people to develop on our base than we could do on our own... With this, any developer worldwide can build full applications on top of the social graph inside the Facebook Platform."<sup>4</sup>

Developers were quick to seize this opportunity. Before Facebook launched the new platform, there were about 100 applications listed in Facebook's developer directory.<sup>5</sup> In less than a year, the number of these "widgets," another name for applications developed by outside developers, exploded to more than 20,000.<sup>6</sup>

This new "Facebook Economy" has been widely heralded as a model for online media and some commentators have even suggested that the company could be "the next Google."<sup>7</sup> Whether or not Facebook achieves that level of success, the new platform has been a golden opportunity for some of the 200,000 developers active on the social network.<sup>8</sup> Although most of these companies are private and financial information is scant, available revenue information for some of the top-performing companies is impressive. One company, [SNAP Interactive](#), the maker of the popular [Are You Interested?](#) application, saw its 4<sup>th</sup> quarter revenues in 2007 jump from \$35,383 to \$388,000, a more than ten-fold increase.<sup>9</sup> [Slide](#), maker of applications [Top Friends](#) and [FunWall](#) and arguably the most successful single developer on Facebook with 4.5 million members<sup>10</sup> using its applications, was valued at \$500 million in January 2008.<sup>11</sup>

Developers aren't the only ones capitalizing on this opportunity. In recent months, numerous venture capital firms, such as Sequoia Capital and Lightspeed Ventures, have invested millions of dollars in companies with Facebook-based businesses. Dozens of social advertising networks have also cropped up, offering widget makers a variety of ways of monetizing their applications, ranging from traditional options like cost-per-click advertising to more unconventional alternatives such as video advertising and lead generation. Facebook itself has profited too. In the last year the number of its members trebled to 67 million, making it the 5<sup>th</sup> most-trafficked website in the world and the 2<sup>nd</sup> largest social networking site.<sup>12</sup>

But while this platform has benefited many, it raises concerns about user privacy. Because of their deep integration into Facebook, developers have extensive access to user information, but it is often unclear if, when and how they exploit this data. This situation is perpetuated by Facebook's unwillingness to regulate the widgets that operate on the site. As a result, users often have no idea who is collecting their data, how information is obtained as one interacts with these applications and how such data – even so-called not non-personally identifiable information – is subsequently used. By eschewing liability and placing the burden of responsibility on developers to police their own applications, Facebook unnecessarily

<sup>1</sup> <http://www.techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/>

<sup>2</sup> <http://www.techcrunch.com/2007/07/06/facebook-users-up-89-over-last-year-demographic-shift/>

<sup>3</sup> <http://www.techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/>

<sup>4</sup> <http://blogs.zdnet.com/BTL/?p=5156>

<sup>5</sup> <http://mashable.com/2007/05/02/10-awesome-things-built-on-the-facebook-api/>

<sup>6</sup> [www.adonomics.com](http://www.adonomics.com)

<sup>7</sup> <http://publishing2.com/2007/05/25/facebook-platform-could-be-a-google-like-market-driven-growth-engine/>

<sup>8</sup> [www.adonomics.com](http://www.adonomics.com)

<sup>9</sup> <http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?capId=11790940>

<sup>10</sup> <http://adonomics.com/company/Slide>

<sup>11</sup> [http://www.businessweek.com/technology/content/jan2008/tc20080118\\_811726.htm?chan=technology\\_technology+index+page\\_top+stories](http://www.businessweek.com/technology/content/jan2008/tc20080118_811726.htm?chan=technology_technology+index+page_top+stories)

<sup>12</sup> <http://www.facebook.com/press/info.php?statistics>

exposes its users to cyber-threats like adware, malware and hackers. In many ways, Facebook has created a dynamic social network, but because of the practices that it has adopted, it needlessly places the privacy and security of its users in harm's way.

### Widget Business Models and Data Issues

Widgets come in many forms. They can be simple games, quizzes, interaction tools or more complex applications that allow users to modify their profiles, compete in fantasy sports leagues and even buy goods and services. But, regardless of their function, the developers that create them almost universally share the same two priorities. First, they try to maximize the number of people that use their widgets. Second, they attempt to leverage this user base to make money.

There are nearly as many ways to monetize a widget as there are kinds of widgets. The most common means of monetization is advertising. Applications can generate advertising revenue by serving ads from social advertising networks, like [SocialMedia](#) or Google's AdSense, often through a cost-per-click or cost-per-action arrangement. Widgets are occasionally used for branding purposes too. Late last year, Coca Cola's Sprite brand debuted an application called [Sprite Sips](#) that allowed users to create a customizable animated character. Similarly, energy-drink manufacturer Red Bull created a branded version of rock-scissors-paper called [Roshambull](#).

Besides advertising and branding, some widgets sell goods and services. [iLike](#), which has received funding from a number of companies, including Ticketmaster, sells downloads to Facebook users, charging record companies a commission for each song that they sell.<sup>13</sup> Other widgets are simply built to attract an audience (in the parlance of Facebook gurus, "build real estate") and then are sold once they have a sizeable user base. Some widget makers have begun to help other developers' widgets acquire users for a fee. A notable example of this is [RockYou!](#), which has made deals to promote other developers' widgets, collecting 50 cents when a user installs one of those applications based on an ad on a RockYou page.<sup>14</sup>

Perhaps the most complex forms of monetization are data collection and lead generation. Although Facebook's privacy policies don't allow personally-identifiable user data from profile pages to be sent outside of Facebook, some developers have circumvented this rule by serving surveys or giveaways that require users to disclose personal information, which is then sold to marketers and other data aggregators.

Sometimes these offers are broadcast in advertisements. But they are often creatively incorporated into the widgets themselves.

For example, a widget called [\(fluff\)Friends](#) allows users to place a cartoon pet on their profile page, which they create and alter using credits called "munny."<sup>15</sup> It is through this "munny" concept that (fluff)Friends conducts its lead generation activities, which is the process of collecting contact information for potential sales leads.<sup>16</sup> In order to interact with or modify your pet, one must use "munny." The easiest way to get "munny" is to take marketing surveys. Although it is unclear how widespread this practice is, data gathering has been facilitated by a number of popular applications, including [Food Fight!](#), [My Aquarium](#), [Hockey Pool Pro](#) and [Free Condoms](#).

### Privacy and Security Concerns

This imperative for developers to monetize their applications creates a scenario that inherently puts user privacy at risk. To a certain extent, this is predictable and users should be cautious about what information they voluntarily disclose on a social network. However, decisions and policies made by Facebook have aggravated this problem, needlessly increasing the vulnerability of users' personal data.

Facebook performs little oversight of the outside developers whose applications run on the social network. According to its [Developers Terms of Service](#), it claims to have virtually no liability for the applications on its platform.<sup>17</sup> Most developers are individuals or privately owned companies, which infrequently publish information about their business relationships, revenues or, in some cases, their

<sup>13</sup> <http://www.techcrunch.com/2006/12/19/scoop-ticketmaster-poops-133-million-into-ilike/>

<sup>14</sup> [http://www.businessweek.com/print/technology/content/jan2008/tc2008017\\_785524.htm](http://www.businessweek.com/print/technology/content/jan2008/tc2008017_785524.htm)

<sup>15</sup> [http://money.cnn.com/2007/08/22/technology/facebook\\_economy.biz2/index.htm](http://money.cnn.com/2007/08/22/technology/facebook_economy.biz2/index.htm)

<sup>16</sup> [http://en.mimi.hu/marketingweb/lead\\_generation.html](http://en.mimi.hu/marketingweb/lead_generation.html)

<sup>17</sup> <http://developers.facebook.com/terms.php> (cited: April 1, 2008).

identities. For instance, a company called [Zoosk](#) created a dating application of the same name that had nearly 500,000 daily active users in February 2008.<sup>18</sup> In spite of the fact that a 500,000 user base would make Zoosk one of the top 20 applications on Facebook, there is almost no publicly available information about the company. This lack of transparency is more the rule than the exception for developers and their applications.

Similarly, it is often unclear how developers utilize the user information they have access to. Outside developers are privy to an enormous amount of user information. According to Facebook's [Platform Application Terms of Use](#), applications know a user's name, profile picture, gender, birthday, location, political views, hobbies, interests, musical preferences, favorite television shows, relationship status, dating interests and even their summer plans.<sup>19</sup> This level of access often far exceeds what is necessary. According to a [University of Virginia study](#), 90.7 percent of applications are given more access to user information than they need.<sup>20</sup>

It is not always apparent how widget makers use this information. Although Facebook maintains policies ostensibly restricting the flow of user information to third parties, it is not evident how well it polices these rules.<sup>21</sup> [Compare People](#), an application with nearly 580,000 daily active users as of February 2008,<sup>22</sup> was the subject of controversy last year when a blogger hacked into the application and discovered that its developer, [Chainn](#), was breaking the Facebook's *Developer Terms of Service* by sending user information to Google for analysis. Although it was reported that none of this information was personally-identifiable and that it was not intended for long-term retention, it was confirmed by Facebook that this was a breach of the network's rules and Chainn has since stopped this practice.<sup>23</sup> However, two things are disconcerting about this incident. First, Chainn does not seem to have been penalized for this violation of user privacy. Second, as one writer put it, "if it takes a blogger to whistleblow...how many other breaches are going undetected?"<sup>24</sup>

The possible relationship between developers and data aggregation companies also raises concerns about user privacy. This link has been cited by a number of sources, including Jason Bailey of the online advertising network [Millnic Media](#). [During a presentation at a Facebook Developers Garage in October 2007](#),<sup>25</sup> Bailey stated that Millnic Media conducts information gathering and lead generation activities through surveys and promotions that it serves to Facebook developers. He specifically mentions that one of the buyers of this information is the online marketing company Value Click.<sup>26</sup> Independent research by the Center for Digital Democracy has also shown a connection between one Facebook widget, Hockey Pool Pro, and the data collector Experian, a global credit information group.<sup>27</sup> In February 2008, Hockey Pool Pro published a marketing survey from WinningSurveys.com, which is owned and operated by Vente, Inc., a subsidiary of Experian. In the past, the CDD has told the Federal Trade Commission that online sites need to disclose to users exactly what data is being collected, shared, sold, analyzed inc. from user actions. Users must be given the right of affirmatively agree, or opt-in to such data practices.

While this relationship between developers and data aggregators is not a violation of Facebook's terms of use, it is nevertheless worrisome and poses a palpable risk to users' information security. In general, marketers and data collectors have not been the best custodians of personal data. In 2004, a data aggregation company named ChoicePoint failed to prevent criminals from improperly accessing the information of 150,000 U.S. citizens.<sup>28</sup> This security breach resulted in at least 750 cases of identity theft.<sup>29</sup> In March 2008, Value Click was fined \$2.9 million for sponsoring deceptive online advertisements and not

---

<sup>18</sup> <http://adonomics.com/about/6953377468>

<sup>19</sup> [http://developers.facebook.com/user\\_terms.php](http://developers.facebook.com/user_terms.php)

<sup>20</sup> <http://www.cs.virginia.edu/felt/privacy/>

<sup>21</sup> <http://developers.facebook.com/terms.php>

<sup>22</sup> <http://adonomics.com/about/2433486906>

<sup>23</sup> <http://venturebeat.com/2007/11/15/more-about-the-google-ads-that-run-inside-facebook/>

<sup>24</sup> <http://venturebeat.com/2007/11/16/google-confirms-adsense-ads-security-problems-with-facebook-applications/>

<sup>25</sup> [http://www.youtube.com/watch?v=MIztj\\_2DcRs&feature=related](http://www.youtube.com/watch?v=MIztj_2DcRs&feature=related)

<sup>26</sup> <http://www.youtube.com/watch?v=t6vjKo6Lzg4> (Around minute 7:00)

<sup>27</sup> See Millnic Media appendix

<sup>28</sup> [http://money.cnn.com/2005/02/28/pf/saving/willis\\_tips/](http://money.cnn.com/2005/02/28/pf/saving/willis_tips/)

<sup>29</sup> [http://www.news.com/Break-in-costs-ChoicePoint-millions/2100-7350\\_3-5797213.html](http://www.news.com/Break-in-costs-ChoicePoint-millions/2100-7350_3-5797213.html)

sufficiently securing customers' personal information. To date, this was the largest CAN-SPAM settlement since the law was enacted in 2003.<sup>30</sup>

In addition to the questions arising from developers' use of personal data, Facebook members face threats from malware and hackers. In January 2008, it was discovered that a company called [Zango](#) was bundling adware with its application, Secret Crush, which informed users that one of their friends had a "crush" on them. The application asked users to reveal personal information and were eventually prompted to install a "Crush Calculator," which is in fact Zango's ad-serving software.<sup>31</sup> Although Facebook disabled the Secret Crush by the end of January, Fortinet, a network security firm stated that four percent of Facebook users had already installed the application.<sup>32</sup>

This incident is not an isolated case. Other bloggers and commentators have reported scattered incidents of unidentified adware distributors on Facebook.<sup>33</sup> This danger is so palpable that Richard Stiennon, a leading commentator on computer and network security, predicts that Facebook widgets distributing malware virus will be the number one emergent threat on the internet in 2008. He states that "we will see attempts to exploit Facebook through these widgets. It could be through a vulnerability in an existing application that could for instance allow the download of a malicious Trojan. Or, it could be a new application deployed to steal information or infect visitors' computers."<sup>34</sup>

### **Will Facebook face up to ensuring privacy protections?**

Through its policies and practices, it is evident that Facebook would prefer to take a *laissez-faire* approach to privacy issues, enjoying the benefits of its social network while doing little to regulate it. It all but states this outright in its *Developers Terms of Service*, where it claims to have virtually no liability for the applications on its platform and charges outside developers with the responsibility to "accurately and adequately disclose" how they "collect, use, store, and disclose data collected from visitors, including, where applicable, that third parties (including advertisers) may serve content and/or advertisements and collect information directly from visitors."<sup>35</sup>

Recently, public concern about the security of user information has compelled Facebook to become more responsive to privacy issues. Last year, the company revised its Beacon initiative, a controversial online ad system that collected information about Facebook member activities on third party sites in order to facilitate targeted advertising. In March 2008, the company introduced new privacy controls that gave users the ability create and manage lists of friends that are granted different levels of access to personal information.<sup>36</sup>

Despite these gestures, Facebook has not done enough. Before a widespread public outcry against the Beacon system, which included a major campaign by MoveOn.org and the petition of almost 70,000 Facebook users,<sup>37</sup> the company showed little regard for user privacy. Similarly, its new user controls are inadequate. Less than a week after these privacy settings were instituted, *The Associated Press* reported that a Canadian computer technician had successfully circumvented them and accessed restricted personal data.<sup>38</sup>

Facebook must do more to guarantee the security and privacy of its members' information. First, it should ensure that developers comply with basic standards of disclosure about who they are, what user information they collect and how they use it. It should be necessary for users to give permission to each application to collect information, once they are told what data is collected and how it is used. Furthermore, Facebook should actively police the network, identifying malicious or other vulnerable widgets that could compromise information security on the site.

---

<sup>30</sup> <http://www.pcmag.com/article2/0,2704,2277079,00.asp>

<sup>31</sup> <http://www.webpronews.com/topnews/2008/01/04/zangos-got-a-secret-crush-on-facebook>

<sup>32</sup> [http://www.theregister.co.uk/2008/01/08/facebook\\_blocks\\_secret\\_crush/](http://www.theregister.co.uk/2008/01/08/facebook_blocks_secret_crush/)

<sup>33</sup> <http://www.scmagazineus.com/Ads-on-Facebook-serve-up-adware/article/35672/>;  
[http://explabs.blogspot.com/2007\\_09\\_01\\_archive.html](http://explabs.blogspot.com/2007_09_01_archive.html)

<sup>34</sup> <http://blogs.zdnet.com/threatchaos/?p=496>

<sup>35</sup> <http://developers.facebook.com/terms.php>

<sup>36</sup> [http://www.washingtonpost.com/wp-dyn/content/article/2008/03/18/AR2008031801983\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/03/18/AR2008031801983_pf.html)

<sup>37</sup> <http://www.commondreams.org/archive/2007/12/06/5640/>

<sup>38</sup> [http://news.yahoo.com/s/ap/20080325/ap\\_on\\_hi\\_te/facebook\\_public\\_photos](http://news.yahoo.com/s/ap/20080325/ap_on_hi_te/facebook_public_photos)

Second, Facebook should make access to user information by applications contingent on a need-to-know basis. Most applications don't require direct access to user data. In many cases, having the ability to access this data puts Facebook users at unnecessary risk. A possible solution to this problem could be a "privacy-by-proxy" system, a data-hiding scheme proposed by researchers at the University of Virginia. These researchers have suggested that developers be given fake "placeholder" data instead of real user information. They state that "this is possible because Facebook has control over the output of applications. When the fake placeholder data is displayed by the application, Facebook can turn it back into the real information for the viewer to see it correctly. Users can be made anonymous with this scheme and third party developers never get to see user information."<sup>39</sup>

Third, there should be an investigation by the FTC and state attorney generals into the link between Facebook applications and data collectors. Although lead generation is a legal business activity, Facebook members should be aware of how their personal information is being used and who is storing it for what purposes.

By opening itself up to outside developers, Facebook is a rich and dynamic social network that is in many ways valued by its users. The 67 million Facebook members are plain evidence of this fact. However, this vibrant online community also represents a threat to its user privacy. Facebook can and should do more to ensure privacy and the security of their personal information.

*Adam Mayle is a freelance writer based in the Northeastern United States.*

---

<sup>39</sup> <http://www.cs.virginia.edu/felt/privacy/>